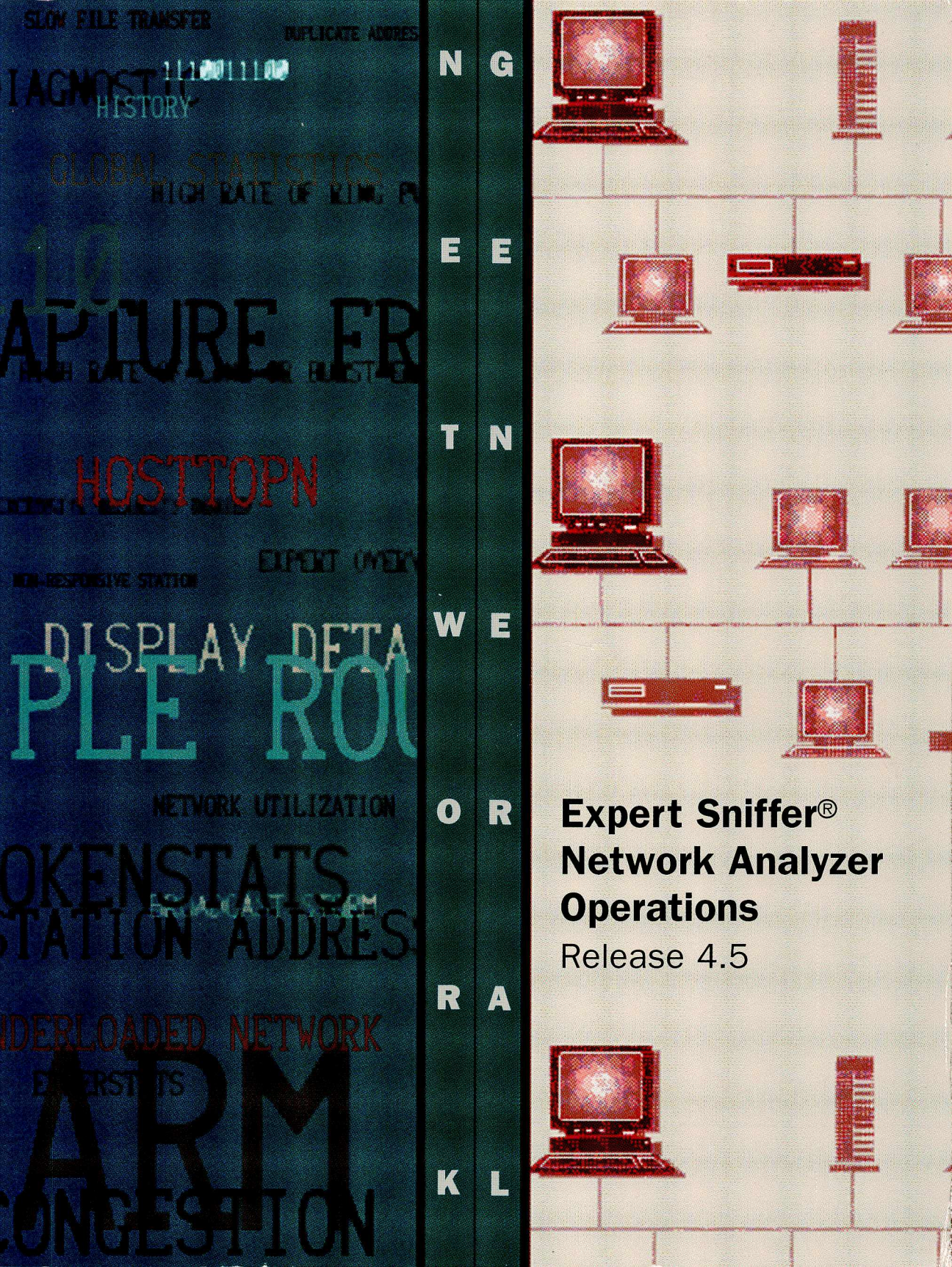
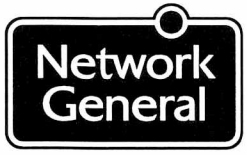


Expert Sniffer® Network Analyzer Operations

Release 4.5

Expert Sniffer® Network Analyzer Operations



Network General, Sniffer, and SniffMaster are registered trademarks of Network General Corporation and/or its wholly owned subsidiaries. All other registered and unregistered trademarks in this document are the sole property of their respective owners. All specifications may be changed without notice.

© 1995 by Network General Corporation. All rights reserved.

January 1995

P/N: 3006002

Table of Contents

Preface

About This Manual xxxv
Organization of This Manual xxxv
Audience of This Manual xxxvi
Navigational Aids Used in This Manual xxxvi
Warning Box xxxvii
Conventions Used in This Manual xxxvii
Special Notations xxxvii
Terminology xxxviii
Screen Displays xxxviii
Other Sources of Information xxxviii
Manuals for the Sniffer Network Analyzer xxxviii
Online Help xxxix
Technical Support xl
Training xl

Chapter 1. Sniffer Network Analyzer Overview

Overview 1-3
Major Components of the Sniffer Network Analyzer 1-3
Conceptual Overview of Sniffer Analyzer Functions 1-4
The Analyzer as (Mostly) Passive Observer 1-5
A Map of the Analyzer's Functions 1-6
Starting the Sniffer Analyzer 1-8
New Features of the Expert Analyzer 1-11
Overview of the User Interface 1-12
Using the Function Keys 1-12
Tree-Structure of the Analyzer's Menus 1-13
Using a Mouse with the Analyzer 1-14

Chapter 2. Getting Familiar with the Expert Analyzer

Overview 2-3
Expert Analyzer Terminology 2-3
About Network Objects 2-3
About Symptoms 2-4
About Diagnoses 2-4
Capturing and Analyzing Frames in Expert Mode 2-5
About the Expert Window 2-7
Getting More Information About a Diagnosis 2-8
Getting Context-Sensitive Explain Messages 2-10
User Explain Messages 2-12
Overview 2-12
Setting Up User Explain 2-12
Editing the User Explain Files 2-13
Displaying the User Explain Messages 2-14
Getting More Information About Symptoms and Network Objects 2-16
Protocols Available for Expert Analysis 2-20

Chapter 3. Defining System Options and Scheduled Events

Overview 3-3
Setting the Language Option 3-4
Setting the Audible Clicks Option 3-5
About the Interpret RI Option 3-5
RI Fields and "Data Relative" vs. "Frame Relative" Options 3-6
Effects of Enabling "Interpret RI" 3-6
Effects of Disabling "Interpret RI" 3-7
Setting the Cable Test Option for Ethernet 3-7
Resetting all Options 3-7
Setting the Transceiver Option for the IBM PS/2 Model P/70 3-8
Setting the Token Ring Options 3-8
Setting the Token Ring Speed 3-10
Token Ring Remove Option for Token Ring-1 Analyzer 3-11
Force Open Option for the Token Ring-II Analyzer 3-12
Setting the Sniffer Internetwork Analyzer Options 3-12

Frame Type Options 3-13
Encoding Options 3-14
Line Interface Options 3-15
Setting the FDDI Options 3-17
Setting the Station Mode 3-17
Inverting Addresses 3-18
Scheduled Events 3-19
Overview 3-19
The Scheduled Events Table 3-19
Choosing When an Event Occurs 3-21
Scheduling Events in Greenwich Mean Time 3-22
Choosing What Actions are Performed 3-22
Save CSV 3-23
Save trace 3-23
Reset statistics 3-24
Clear names 3-24
Load names 3-24
Load setup file 3-24
Updating the Scheduled Events Table 3-24
The SCHEDULE.CFG File 3-25

Chapter 4. Defining Expert Analyzer Options

Overview 4-3
Expert Layers and the OSI Model 4-4
Configuring the Expert Analyzer 4-7
Setting Subnet Masks 4-7
Example: Using an Incorrect Subnet Mask 4-8
Setting Trustee Names 4-12
Setting Thresholds for Symptoms and Diagnoses 4-13
Symptom and Diagnosis Thresholds at Each Expert Layer 4-16
How the Expert Thresholds Interact 4-16
Application Thresholds 4-18
Minimum Application Requests 4-18
Response Time 4-18

Slow Response Percentage 4-18
Filter Time 4-19
Denied Count 4-19
Loop Percentage 4-20
Denied Request Percentage 4-20
Local Transfer/ Remote Transfer 4-21
Slow File Percentage 4-21
Connection Thresholds 4-22
No Responses 4-22
Retransmission Percentage 4-22
Zero Window 4-22
Idle Timer 4-23
Fast Retransmission 4-23
TCP Keep Alive 4-23
DEC Keep Alive 4-23
PAP Wait 4-24
Network Station Thresholds 4-24
Multiple Routers 4-24
DEC Hello 4-24
Duplicate Percentage 4-24
DLC Station Thresholds 4-25
LAN Overload 4-26
LAN Overload Percentage 4-26
Broadcast Symptom 4-27
Broadcast Diagnosis 4-27
ZIP Storm 4-27
Physical Errors 4-28
Token Ring-Specific (MAC layer) Thresholds 4-28
Ring Entries 4-28
RX Congestion (Receiver Congestion) 4-28
Station Removed 4-29
Ring Errors 4-29
Ring Purge Symptom 4-29
Ring Purge Diagnosis 4-30
WAN/Synchronous (Sniffer Internetwork Analyzer) Thresholds 4-30
WAN Overload 4-30
Overload Timer 4-31
WAN Underload 4-31

Underload Timer 4-31
Congestion Percentage 4-32
Effects of Changing Expert Thresholds 4-32
Example One: Changing a Threshold Irrelevant to the Data in the Capture Buffer 4-33
Example Two: Changing a Threshold Relevant to the Data in the Capture Buffer 4-34
Customizing a Capture Session 4-35
Recycle Objects Option 4-35
How the Expert Analyzer Reuses Network Objects 4-36
Name Width Display Option 4-37
How the Expert Analyzer Learns Symbolic Names 4-37

Chapter 5. Expert Analyzer Capture and Display

Overview 5-3
Displaying Analysis Results In the Expert Window 5-3
Navigating the Expert Window 5-6
The Expert Overview Display 5-8
Navigating through the Expert Overview 5-9
Other Counters in the Expert Overview 5-9
Diagnosis-Related Displays 5-10
Diagnosis Summary Window 5-10
Temporarily Removing Diagnoses From the Expert Window 5-12
Diagnosis Detail Displays 5-14
Broadcast Storm 5-16
Duplicate Network Address 5-17
Excessive Repeated Requests 5-18
Excessive Requests Denied 5-19
File Overlap / Retransmission 5-21
High Rate of Congestion 5-22
High Rate of Line or Burst Errors 5-23
High Rate of Physical Errors 5-23
High Rate of Remove from Ring Requests 5-24
High Rate of Ring Entries 5-26
High Rate of Ring Purges 5-27
LAN Overloaded 5-28

Local Router 5-29
Multiple Routers to Station 5-30
Non-Responsive Station 5-31
Retransmissions 5-33
Ring Beaconing 5-34
Slow File Transfer 5-35
Slow Server 5-36
Underloaded Network 5-37
Symptom and Network Object-Related Displays 5-38
About Symptom and Network Object-Related Displays 5-38
Symptom and Network Object Summary Windows 5-38
Displaying the Summary Window 5-39
Information in the Summary Windows 5-40
Information Fields in the Summary Windows 5-41
Changing the Format of the Summary Window 5-43
Application and Connection Layer Summary Window 5-44
Network Station Summary Window 5-46
DLC Station Summary Window 5-48
Subnet Pairs Summary Window 5-49
Global Symptom Summary Window 5-50
Symptom and Network Object Detail Windows 5-52
Displaying the Detail Window 5-52
Information in the Detail Windows 5-54
Subnet Pairs Detail Window 5-56
Global Symptom Detail Window 5-58
Information in the Global Symptom Detail Window 5-60
Symptom and Network Object Statistics Windows 5-60
Displaying a Statistics Window 5-61
Application Statistics Window 5-63
Connection Statistics Window 5-65
Network Station Statistics Window 5-67
DLC Station Statistics Window 5-68
The Global Statistics Window 5-72
Composition of the Global Statistics Window 5-73
Composition of Traffic by Protocol Family 5-73

Percentage Bandwidth Utilization 5-74
Run Information 5-74
Effects of Capture Filters on Global Statistics 5-76
Effects of Frame Size Option on Global Statistics 5-76
Advanced Navigation Techniques 5-77
Using the Higher Layer/Lower Layer Function Keys 5-77
Using the Next Symptom/Previous Symptom Keys 5-79
Function Keys in the Expert Window 5-80

Chapter 6. Capturing Frames

Overview 6-3
Capture Menu Overview 6-3
Ethernet Cable Tester 6-4
Automatic Test at First Capture 6-5
Messages Provided by the Cable Tester 6-5
Limitations of the Cable Tester 6-6
Displaying Information About the Capture Buffer 6-6
Preparing to Capture Frames: An Overview 6-8
Choosing a Capture Mode 6-10
Defining the Basic Capture Options 6-10
Defining Frame Size during Capture 6-10
Defining the Capture Source: Live Network or Data File 6-11
Limitations of Capturing from a Saved Trace File 6-12
Defining Screen Format During Capture: An Overview 6-13
Screen Formats for LANs During Capture 6-13
Screen Formats for WAN/Synchronous Networks During Capture . 6-14
Defining the Screen Format During Capture: Procedure 6-14
Information in the Tabular Views 6-17
Counters 6-18
Buffer Utilization 6-19
Station Names 6-19
Pair Counts During Capture: LAN 6-19
Information in the Skyline View 6-28
Counters 6-28
Buffer Utilization 6-29

Skyline Views for LAN Networks 6-29
Skyline Views for WAN/Synchronous Networks 6-30
Choosing Highspeed Capture Mode 6-32
Setting the Capture Filters 6-33
Saving Selected Capture Filters 6-36
Disabling the Capture Filters 6-36
Capture Filters and the Name Table 6-37
Known Stations Only Filter 6-38
Unknown Stations Only Filter (LAN) 6-38
Destination Class Filter 6-38
Station Address Filters 6-39
Defining Station Address Matches: Some Considerations 6-40
Defining the Station Address Filters 6-41
Protocol Filter 6-43
Pattern Match Filter 6-45
Four Contexts for Pattern Matching 6-45
Defining Complex Pattern Matches 6-46
Logical Combinations of the Four Matches 6-47
Pairs of Patterns within a Match 6-48
Temporarily Disabling a Match 6-48
A Match on a Pair of Patterns 6-48
Effect of the Either Offset Option 6-49
Effect of the Match/Don't Match Option 6-50
Characters and Offset in an Individual Pattern 6-51
Data-Relative vs. Frame-Relative Offset 6-51
Defining a Pattern Match Filter 6-52
Copying and Pasting a Pattern from the Display Hex Window 6-55
Example of a Capture Filter Pattern Match 6-55
Void/Claim Frames Filter 6-57
Filters for Defective Frames 6-58
How the Defective Frames Filters Work (Ethernet) 6-58
Defective Frames on an FDDI Network 6-59
Sniffer Internetwork Analyzer Capture Filters 6-60
From DTE/From DCE Capture Filters 6-60
RR Frames/RNR Frames Capture Filters 6-60
Info Frames Capture Filter 6-61

Stopping Capture 6-61
Defining a Trigger to Stop Capture 6-62
Defining the Trigger Event 6-63
Saving the Trigger Frame to Disk 6-66
Defining the Trigger Delay 6-68
Temporarily Disabling the Trigger Option 6-69
Expert Triggers 6-69
Effects of an Expert Trigger 6-71
Available Expert Triggers 6-71
The Order in Which the Analyzer Processes Triggers 6-73
Example: Processing Expert and Classic Triggers 6-73
Starting the Capture 6-74
Pausing or Stopping Capture 6-74
What You Can Do While Capture is Paused 6-74
What You Can Do When Capture Has Stopped 6-75

Chapter 7. Displaying Interpreted Frames

Overview 7-3
Display Menu Overview 7-3
Role of the Capture Buffer in Displaying Frames 7-4
Setting the Display Filters 7-4
Overview of Available Filters 7-5
Procedure: Specifying the Display Filters 7-7
Address Level Filter 7-8
Effect on Displayed Frames 7-10
Destination Class Filter 7-10
Station Address Display Filter 7-11
Considerations when Setting Address Filters 7-14
Adding Addresses to the Name Table 7-14
Protocol Display Filter 7-14
Pattern Match Display Filter 7-15
Selected Frames Display Filter 7-16
Filters for Defective Frames 7-16
Expert Display Filters 7-17

Network Object Filter 7-17
Symptom Frames Filter 7-24
Disabling the Display Filters 7-26
Displaying Interpreted Frames 7-27
The Display Options: An Overview 7-27
About the Use of Color 7-29
Scrolling within the Display Views 7-30
Moving between the Display Views 7-31
Enlarging a Display View 7-32
Compensation for Bit-Reversal in PC Network Addresses 7-32
Compensation for Bit-Reversal in FDDI Networks 7-32
The Summary View 7-33
Numeric Addresses in the Summary View 7-33
Display of Manufacturers' IDs 7-34
Name Width Display Option 7-34
The Summary View Display Options 7-35
All Layers Display Option 7-36
DLC Addresses Display Option 7-38
Manufacturers' IDs Display Option 7-38
Two-Station Format Display Option 7-39
Flags Display Option 7-40
"Time" and "Volume" Display Options 7-41
The Detail View 7-44
Protocol Layers in the Detail View 7-45
Scrolling in the Detail View 7-45
Formats for Higher-Level Numeric Addresses 7-46
The Hexadecimal View 7-47
Display of Spanned Frames 7-49
The Hexadecimal View Display Options 7-51
Defining the Type of Interpretation 7-51
Selecting ASCII Parity 7-51
Function Keys Available During Display 7-51
Using Hexadecimal View to Edit Frames 7-53
Searching for Frames 7-55
Searching for a Frame Number 7-56
Searching for Text 7-57

Searching for a Pattern 7-59
Jumping to the Marked Frame 7-60
Jumping to the Trigger Frame 7-60
Printing and Importing Data 7-60
Defining the Range of Frames 7-63
Defining the Destination: Printer or File 7-63
Defining the File Format 7-64
Choosing Page Titles 7-65
Choosing Page Size 7-66
Background Information: Protocol Interpretation 7-66
Transmission of 6-Byte DLC Addresses 7-66
Bits on the Wire vs. Bits in Memory 7-66
Consequence of the IEEE standard 7-67
Protocol Interpretation 7-67
Bit-Level Interpretation 7-67
Alternate Displays for ASN.1-Encoded Protocols 7-68
Token Ring and FDDI Trailer Byte 7-71

Chapter 8. Managing Names and Working with Files

Overview 8-3
Managing Names 8-3
About the Name Table 8-4
How the Analyzer Builds the Name Table 8-5
Taking Advantage of the Automatic Address Scan 8-6
Assigning Names to Addresses 8-6
Manually Editing the Name Table 8-7
Using Name Files to Resolve Names 8-9
Looking for Names in Captured Frames 8-10
Saving the Name Table 8-10
Clearing the Name Table 8-11
Saving Captured Frames as Data (Trace) Files 8-11
Converting Internetwork Analyzer Trace Files to LM2000 Format 8-13
Using the Sniffer—LM2000 Conversion Utility 8-13
Using Data Files to Load the Capture Buffer 8-16
Deleting Data Files 8-18

Saving Expert Data 8-18
Using Setup Files to Define System Options 8-21
Contents of a Setup File 8-21
Saving the Current Options in the STARTUP File 8-22
Saving the Current Options as a Setup File 8-23
Applying a Setup File 8-23
Restoring the Network General Default Options 8-23

Chapter 9. Using Protocol Forcing

Overview 9-3
How Protocol Forcing Works 9-3
Specifying a Protocol Forcing Rule 9-4
Applying a Protocol Forcing Rule 9-10
Disabling Protocol Forcing 9-13
Special Considerations for Protocol Forcing 9-14

Chapter 10. Generating Traffic

Overview 10-3
Traffic Generator Menu Overview 10-4
Preparing to Generate Traffic: Single Frame Mode 10-5
Specifying Destination 10-5
Specifying Frame Size 10-5
Specifying the Delay Between Generated Frames 10-6
Specifying the Number of Frames to Generate 10-7
Defining the Frame's Data Field 10-7
Structure of a Generated Frame 10-8
Specifying the RI Bit in Generated Frames 10-9
Preparing to Generate Traffic: Buffer Mode 10-11
Starting and Stopping Traffic Generation 10-13
Example: Format of the Generated Frame 10-14

Chapter 11. The Analyzer's File System

Overview 11-3
About File Names and Extensions 11-3

The Sniffer Analyzer Directories and Files 11-6
Root Directory 11-6
DOS Directory 11-6
TOOLS Directory 11-7
CONFIG Directory 11-7
xxSNIFF Directory 11-7
Files and Subdirectories within the xxSNIFF Directory 11-7
xxREPORT Directory 11-8
CAPTURE Directory 11-8
REMOTE2 Directory 11-8
Configuring the Remote^2 Host 11-8
Working with Files 11-9
Creating Alternate Directories for Saved Files 11-9
Setting the Path to a Directory for Saved Files 11-10
STARTUP Files 11-10
Modifying the STARTUP.xxS File 11-12
Restoring the Factory Defaults 11-13
About the Name Tables 11-13
Creating Name Files 11-14
Creating Your Own Name File 11-14
Name Table with Default Types 11-16
Table of Manufacturer ID Codes and Abbreviations 11-16
File Formats 11-18
Format of Saved Data Files 11-18
Structures within the Data File 11-19
The Startup Parameters 11-21
Automatic Restart Option 11-21
How the Parameters are Passed 11-22
Editing the Startup Parameters 11-22
Startup Parameters List 11-23

Appendix A. Symptom and Diagnosis Messages

Overview A-3
Symptoms A-3

Application Layer A-3
Connection Layer A-4
Network Station Layer A-7
DLC Station Layer A-11
MAC Layer (Token Ring) A-11
WAN/Synchronous A-13
Diagnoses A-16
Application Layer A-16
Connection Layer A-17
Network Station Layer A-17
DLC Station Layer A-18
MAC Layer (Token Ring) A-18
WAN/Synchronous A-19

Appendix B. Troubleshooting Guide

Communicating with Network General Corporation B-4
Using FTP B-4
Using CompuServe B-5
Accessing Sniffnet BBS B-5
Troubleshooting Checklist B-6

Index

List of Figures

Preface

Figure i. Scope of each chapter and appendix xxxv
Figure ii. Manuals for the Sniffer Network Analyzer xxxviii
Figure iii. Technical support contact information xl

Chapter 1. Sniffer Network Analyzer Overview

Figure 1–1 Major software components of the Sniffer Network Analyzer 1-3
Figure 1–2. Overview of Sniffer analyzer functions. 1-7
Figure 1–3. Main Selection Menu of the Sniffer Network Analyzer 1-8
Figure 1–4. Initialization screen of the Sniffer Network Analyzer 1-9
Figure 1–5. Main Menu of the Sniffer analyzer (Ethernet). 1-10
Figure 1–6. New features of the Expert Sniffer analyzer 1-11
Figure 1–7. Function keys available during capture 1-12
Figure 1–8. Main menu of the Sniffer analyzer (in this case, for Ethernet) 1-13
Figure 1–9. Mouse functions 1-16

Chapter 2. Getting Familiar with the Expert Analyzer

Figure 2–1. Main Menu of the Sniffer analyzer (in this case, for Ethernet) 2-6
Figure 2–2. Expert Overview window of the Expert analyzer 2-7
Figure 2–3. Application Diagnosis Summary window. 2-9
Figure 2–4. Application Diagnosis Detail screen 2-10
Figure 2–5. Explain screen for the diagnosis *Slow server* 2-11
Figure 2–6. Context-sensitive user explain templates. 2-13
Figure 2–7. Adding a user explain message to the GLOBAL.TPL file 2-14
Figure 2–8. User explain text for the LAN overload symptom. 2-15
Figure 2–9. Expert Overview screen 2-16
Figure 2–10. Connection Summary window. 2-17
Figure 2–11. Connection Detail window 2-18
Figure 2–12. Connection Statistics screen 2-19
Figure 2–13. Protocols currently available for Expert analysis 2-20

Figure 2–14. The protocols on which the analyzer can perform Expert analysis . 2-21

Chapter 3. Defining System Options and Scheduled Events

Figure 3–1. The Options menu for the Ethernet analyzer. 3-4
Figure 3–2. The Options menu for the token ring analyzer 3-9
Figure 3–3. Setting the token ring speed. 3-10
Figure 3–4. The Options menu: WAN/Synchronous analyzer 3-13
Figure 3–5. FDDI options. 3-17
Figure 3–6. Show LLC or SMT addresses option 3-19
Figure 3–7. The scheduled events table. 3-20
Figure 3–8. Three schedule modes. 3-21
Figure 3–9. Types of scheduled events. 3-22

Chapter 4. Defining Expert Analyzer Options

Figure 4–1. How the OSI model of network layers relates to the Expert model. . . 4-5
Figure 4–2. The Diagnosis Overview window. 4-6
Figure 4–3. Expert config menu of the Expert Sniffer analyzer. 4-7
Figure 4–4. Two different Class A IP broadcast addresses 4-8
Figure 4–5. Set Subnet Masks box. 4-9
Figure 4–6. Entering the IP network address. 4-10
Figure 4–7. Entering the associated subnet mask 4-10
Figure 4–8. List of defined IP network addresses and subnet masks 4-10
Figure 4–9. Modifying or deleting the IP address 4-11
Figure 4–10. Set Trustee Names box. 4-12
Figure 4–11. Entering a new Trustee Name 4-13
Figure 4–12. The Expert config\Thresholds\Connection layer menu 4-15
Figure 4–13 Expert thresholds available at each Expert layer. 4-17
Figure 4–14. How the analyzer calculates Duplicate address percentage 4-25
Figure 4–15. The relationship between*LAN overload* and *LAN overload%* 4-27
Figure 4–16. Results of Expert analysis can vary depending on when performed. 4-33
Figure 4–17. A single frame with two symptoms. 4-35

Chapter 5. Expert Analyzer Capture and Display

Figure 5–1. Expert analyzer displays 5-4
Figure 5–2. The Expert Overview 5-8
Figure 5–3. Diagnosis Summary window 5-11
Figure 5–4. Diagnosis detail displays and expert thresholds 5-15
Figure 5–5. Detail display for the diagnosis *Broadcast storm* 5-16
Figure 5–6. Detail display for the diagnosis *Duplicate net address* 5-17
Figure 5–7. Detail display for the diagnosis *Excessive repeated requests* 5-19
Figure 5–8. Detail display for the diagnosis *Excessive requests denied* 5-20
Figure 5–9. Detail display for the diagnosis *File overlap/retransmission* 5-21
Figure 5–10. Detail display for the diagnosis *High rate of congestion* 5-22
Figure 5–11. Detail display for the diagnosis *High rate of line/burst errors* 5-23
Figure 5–12. Detail display for the diagnosis *High rate of physical errors* 5-24
Figure 5–13. Detail display for *High rate of remove from ring requests* 5-25
Figure 5–14. Detail display for the diagnosis *High rate of ring entry* 5-26
Figure 5–15. Detail display for the diagnosis *High rate of ring purges* 5-27
Figure 5–16. Detail display for the diagnosis *LAN overloaded* 5-28
Figure 5–17. Detail display for the diagnosis *Local Router* 5-29
Figure 5–18. Detail display for the diagnosis *Multiple routers to station* 5-30
Figure 5–19. How the analyzer calculates a broken connection 5-31
Figure 5–20. Detail display for the diagnosis *Non-responsive station* 5-32
Figure 5–21. Detail display for the diagnosis *Retransmissions* 5-33
Figure 5–22. Detail display for the diagnosis *Ring beaconing* 5-34
Figure 5–23. Detail display for the diagnosis *Slow file transfer* 5-35
Figure 5–24. Detail display for the diagnosis *Slow server* 5-36
Figure 5–25. Detail display for the diagnosis *Underloaded network* 5-37
Figure 5–26. Symptom and Network Object Summary window 5-39
Figure 5–27. Network Station Summary window 5-41
Figure 5–28. The default Application Summary window 5-44
Figure 5–29. Application and Connection layer Summary window formats 5-45
Figure 5–30. Application Summary window in DLC station format 5-45
Figure 5–31. Connection Summary window in Protocol format 5-46
Figure 5–32. Network Station Summary window 5-47

Figure 5–33. Network Station layer Summary window formats 5-47
Figure 5–34. DLC Station Summary window 5-48
Figure 5–35. DLC Station Summary window formats. 5-48
Figure 5–36. Subnet Pairs Summary window 5-50
Figure 5–37. Global Symptom Summary window. 5-51
Figure 5–38. Application Detail window 5-52
Figure 5–39. Network Station Detail window. 5-54
Figure 5–40. How the analyzer interprets the DLC name and address 5-56
Figure 5–41. Subnet Pairs Detail Window 5-57
Figure 5–42. Global Symptom Detail window 5-59
Figure 5–43. Application Statistics window 5-63
Figure 5–44. How the Expert analyzer calculates the value for Interframe time . 5-65
Figure 5–45. Connection Statistics window (in this case, for TCP/IP) 5-66
Figure 5–46. Network Station Statistics window 5-67
Figure 5–47. DLC Station Statistics Window. 5-69
Figure 5–48. The Global Statistics window. 5-72
Figure 5–49. Application Summary screen with F7 (Lower layer) visible 5-78
Figure 5–50. Pop-up box for selecting related network station to display 5-79

Chapter 6. Capturing Frames

Figure 6–1. Overview of the Capture menu options 6-4
Figure 6–2. Displaying memory statistics. 6-7
Figure 6–3. Preparing for capture: an overview. 6-9
Figure 6–4. Effect of high-level frames spanning multiple DLC frames 6-11
Figure 6–5. Choosing the capture source. 6-12
Figure 6–6. Summary of screen formats for most LANs 6-13
Figure 6–7. Effect of various screen format options. 6-14
Figure 6–8. Capture menu options for frames, kilobytes, and usage 6-16
Figure 6–9. Traffic density bar graph for LANs (logarithmic scale) 6-16
Figure 6–10. Traffic density bars for WAN/Synchronous link 6-16
Figure 6–11. Sample tabular Ethernet display: pair counts 6-17
Figure 6–12. Sample tabular FDDI display: pair counts 6-18
Figure 6–13. Sample tabular view: pair counts 6-20
Figure 6–14. Sample tabular view: individual counts 6-21

Figure 6–15. Internetwork Analyzer capture view: Frame relay access protocol . 6-25
Figure 6–16. Internetwork Analyzer capture view: X.25/HDLC access protocol . 6-26
Figure 6–17. Sample LAN skyline view 6-29
Figure 6–18. Sample WAN/Synchronous skyline view 6-30
Figure 6–19. Information displayed during capture in Highspeed mode 6-32
Figure 6–20. Setting the Ethernet capture filters 6-33
Figure 6–21. Overview of available LAN capture filters. 6-34
Figure 6–22. Overview of Sniffer Internetwork Analyzer capture filters 6-35
Figure 6–23. The working name table. 6-37
Figure 6–24. Formats of generic addresses, by network of origin. 6-39
Figure 6–25. Address filter to capture all traffic from a station. 6-41
Figure 6–26. Example of a filter match on three address pairs 6-41
Figure 6–27. Defining a station address capture filter. 6-42
Figure 6–28. Selecting a station for a station address filter. 6-42
Figure 6–29. Entering a new station address and name. 6-43
Figure 6–30. Defining the protocol capture filters 6-44
Figure 6–31. DLC protocols typically available for capture filters 6-45
Figure 6–32. Defining a pattern match 6-47
Figure 6–33. Combining four matches with AND and OR 6-48
Figure 6–34. Frame containing both A at a AND B at b 6-49
Figure 6–35. Frames containing either A at offset a OR B at offset b. 6-49
Figure 6–36. Effect of "Either offset" option 6-50
Figure 6–37. Effect of "Either offset" when pairs are linked by OR 6-50
Figure 6–38. Defining a pattern match 6-53
Figure 6–39. Example of a pattern match in the capture filter 6-57
Figure 6–40. Collision detection 6-59
Figure 6–41. Overview of how collision frames are treated 6-59
Figure 6–42. Indication that capture is stopped by trigger event 6-62
Figure 6–43. Trigger menu for an Ethernet-II analyzer. 6-64
Figure 6–44. Sample trigger pattern matches 6-65
Figure 6–45. Defining the size of snapshot files. 6-67
Figure 6–46. Effect of "stop capture" options in the trigger menu 6-68
Figure 6–47. The Trigger\Expert trigger\Application layer menu 6-70

Figure 6–48. The Trigger\Expert trigger\Application layer menu 6-72
Figure 6–49. The order in which the analyzer processes triggers 6-73
Figure 6–50. Discarding captured frames 6-76

Chapter 7. Displaying Interpreted Frames

Figure 7–1. Overview of the Display menu options 7-4
Figure 7–2. The display filters 7-5
Figure 7–3. The Display Options menu 7-8
Figure 7–4. Specifying the Address level display filters 7-9
Figure 7–5. Specifying the Destination class display filter 7-11
Figure 7–6. Naming a station address filter match 7-12
Figure 7–7. Selecting a station as a station address filter 7-13
Figure 7–8. Defining a new station as a station address filter 7-13
Figure 7–9. Specifying the Protocol display filters 7-15
Figure 7–10. Setting a Network object filter 7-19
Figure 7–11. Summary display with Network object filter 7-20
Figure 7–12. Network Stations Summary window 7-21
Figure 7–13. Network object filter on the server *BIZ-ONE* 7-21
Figure 7–14. The Display\Filters menu 7-23
Figure 7–15. Displaying the current Network object filter 7-24
Figure 7–16. *Symptom frames* filter 7-25
Figure 7–17. Classic Summary display 7-26
Figure 7–18. Displaying interpreted frames in all three views 7-28
Figure 7–19. Displaying interpreted frames 7-29
Figure 7–20. Colors associated with protocol layers 7-30
Figure 7–21. Synchronized scrolling in the display views 7-31
Figure 7–22. Sample Summary view 7-33
Figure 7–23. The Summary view display options 7-35
Figure 7–24. Summary view, All layers and DLC addresses enabled 7-37
Figure 7–25. Summary view, All layers and DLC addresses disabled 7-38
Figure 7–26. Two-station format for the **Summary** view 7-39
Figure 7–27. Displaying flags in the Summary view 7-40
Figure 7–28. Displaying time and traffic volume information 7-42
Figure 7–29. Sample Detail view 7-44

Figure 7–30. Sample of complete Detail view information when printed 7-45
Figure 7–31. Address formats for selected networks and protocols 7-47
Figure 7–32. Hexadecimal view of a TCP/IP frame on Ethernet 7-48
Figure 7–33. Synchronized highlighting in the Detail and Hex views 7-49
Figure 7–34. **Detail** and **Hex** view of a spanned ISO frame 7-50
Figure 7–35. The Edit options for editing frames 7-54
Figure 7–36. Text search options 7-56
Figure 7–37. Searching the capture buffer for text 7-57
Figure 7–38. Entering text for which to search 7-58
Figure 7–39. Searching the capture buffer for a pattern 7-59
Figure 7–40. Printing and importing data 7-61
Figure 7–41. Portion of a printed report 7-63
Figure 7–42. Delimited format (all levels) 7-65
Figure 7–43. Bit-by-bit interpretation of a byte 7-68
Figure 7–44. Bit-by-bit interpretation of three SNA bytes on token ring 7-68
Figure 7–45. Bit-by-bit interpretation of three SNA bytes on token ring 7-70
Figure 7–46. Detail view 7-71

Chapter 8. Managing Names and Working with Files

Figure 8–1. Managing the name table 8-4
Figure 8–2. Sample working name table 8-5
Figure 8–3. Editing the working name table 8-7
Figure 8–4. Changing an existing name 8-8
Figure 8–5. Entering a station's name and address 8-8
Figure 8–6. Menu to save captured frames to a file 8-12
Figure 8–7. Main Menu of the Sniffer Network Analyzer 8-13
Figure 8–8. Main menu of the LM2000—Sniffer Conversion Utility 8-14
Figure 8–9. Window for specifying trace file to be converted 8-15
Figure 8–10. Dialog box for naming converted trace file 8-16
Figure 8–11. Loading the capture buffer with a data file 8-17
Figure 8–12. Saving Expert data 8-19
Figure 8–13. Choosing network objects 8-20
Figure 8–14. Choosing layers for diagnoses 8-21

Chapter 9. Using Protocol Forcing

Figure 9–1. Protocol forcing menu options 9-4
Figure 9–2. Protocol forcing rule options 9-5
Figure 9–3. Protocol forcing If menu 9-6
Figure 9–4. Select Station address name table 9-7
Figure 9–5. Port option window 9-8
Figure 9–6. Byte offset window 9-9
Figure 9–7. Protocol forcing Then menu 9-10
Figure 9–8. Display without protocol forcing 9-11
Figure 9–9. Protocol forcing rule 9-12
Figure 9–10. Display using protocol forcing 9-13

Chapter 10. Generating Traffic

Figure 10–1. Traffic generator menu options 10-4
Figure 10–2. Size ranges of generated frames 10-6
Figure 10–3. Interval ranges between consecutive generated frames 10-7
Figure 10–4. Structure of a generated frame 10-8
Figure 10–5. Location of the user-definable data in a generated frame 10-10
Figure 10–6. Position of RI field in Ethertype and IEEE 802.3 frames 10-11
Figure 10–7. Using the Traffic generator to transmit the capture buffer 10-12
Figure 10–8. Generating frames on a token ring network 10-13
Figure 10–9. Defining a token ring frame to be generated 10-14
Figure 10–10. Appearance of the generated token ring frame 10-15

Chapter 11. The Analyzer's File System

Figure 11–1. General DOS extensions 11-4
Figure 11–2 Sniffer analyzer extensions 11-5
Figure 11–3. The Sniffer analyzer directories 11-6
Figure 11–4. The Sniffer analyzer startup files 11-11
Figure 11–5. Stored files and working copies of name tables and setups 11-12
Figure 11–6. Sample name file 11-14
Figure 11–7. The name file of Figure 11–6 rewritten with default types 11-16
Figure 11–8. Manufacturer ID translation 11-17

Figure 11–9. Startup parameters that affect use 11-24
Figure 11–10. Startup parameters that affect expanded memory 11-25
Figure 11–11. Startup parameters that report adapter card configuration 11-25

List of Procedures

Chapter 1. Sniffer Network Analyzer Overview

To start the Sniffer analyzer: 1-8
To work with the Sniffer analyzer menus: 1-14
To use online help: 1-14

Chapter 2. Getting Familiar with the Expert Analyzer

To obtain more information about a diagnosis: 2-8
To display an Explain message during capture: 2-11
To view the protocols for which expert analysis is available: 2-20

Chapter 3. Defining System Options and Scheduled Events

To set the Language option: 3-5
To set or clear the Audible clicks option: 3-5
To restore the system defaults: 3-7
To choose between ports on the Model 70: 3-8
To set the network speed used by the analyzer's adapter card: 3-10

Chapter 4. Defining Expert Analyzer Options

To add a specific IP network address and associated subnet mask: 4-9
To modify or delete existing IP network addresses and subnet masks: 4-11
To specify trustee names to be excluded from the Novell name search: 4-12
To delete or modify trustee names: 4-13
To set an Expert threshold: 4-14
To define the Name width option: 4-37
To help the Expert analyzer learn symbolic names: 4-38

Chapter 5. Expert Analyzer Capture and Display

To display a Diagnosis Summary window: 5-10
To remove a diagnosis from the Expert window temporarily: 5-12
To restore removed diagnoses to the display: 5-12

To display a Diagnosis Detail window: 5-14
To display a Summary window at any of the Expert layers: 5-39
To change the format of the Summary window: 5-43
To display a Detail window from the Symptom and Network Object column: . . 5-53
To display a Symptom and Network Object Detail window: 5-53
To display a Statistics window from the Symptom and Network Object column: 5-61
To display a Statistics window from the Diagnoses column: 5-61
To display the Global Statistics window: 5-72
To use the Higher layer/Lower layer function keys: 5-77
To use the Next symptom/Previous symptom keys: 5-79

Chapter 6. Capturing Frames

To test the Ethernet segment for cable faults: 6-5
To check the size of the capture buffer: 6-7
To display a summary of memory statistics: 6-7
To choose a capture mode and the associated options: 6-10
To capture from a file: 6-11
To capture from the network: 6-12
To select the screen format for most LANs: 6-15
To select the screen format for a WAN/Synchronous link: 6-15
To "probe" an ARCNET network: 6-22
To adjust the vertical scales to the best level of detail: 6-31
To adjust the horizontal scales to view earlier intervals: 6-31
To select Highspeed mode: 6-33
To set up the capture filters: 6-35
To save the capture filters setup: 6-36
To temporarily disable all selected capture filters: 6-36
To restrict capture to frames from known stations: 6-38
To restrict capture to frames from unknown stations: 6-38
To select or exclude frames by destination class: 6-39
To define station address capture filters: 6-41
To define a pattern match for a capture filter: 6-53
To enter a pattern by copying and pasting: 6-55

To set the Sniffer Internetwork Analyzer capture filters: 6-61
To determine how to stop the capture: 6-61
To define the trigger event on a LAN: 6-64
To define the trigger event on a WAN/Synchronous link: 6-65
To save snapshot files to disk: 6-67
To define the trigger delay: 6-69
To set an Expert trigger: 6-69
To start capture: 6-74

Chapter 7. Displaying Interpreted Frames

To set display filters before you start the display: 7-7
To change filters (or display options) during the display: 7-7
To set an Address level display filter: 7-9
To set a destination class display filter: 7-11
To set a station address filter for display: 7-12
To define the Protocol display filters: 7-15
To enable only one protocol filter: 7-15
To set up a pattern match filter for display: 7-16
To filter only for selected frames: 7-16
To save selected frames to disk: 7-16
To set filters for good frames or for frame defects: 7-17
To set an automatic Network object filter: 7-18
To display the current Network object filter: 7-22
To remove a Network object filter using the Network object menu item: 7-24
To filter out frames that do not exhibit symptoms: 7-25
To disable all selected display filters temporarily: 7-26
To define the displayed protocol levels in Summary view: 7-38
To use the two-station format: 7-39
To set the level initially displayed in the Detail view: 7-46
To maintain cursor position in the Detail view: 7-46
To select the type of interpretation: 7-51
To edit frames: 7-54
To reinterpret edited frames: 7-55
To go to a frame number: 7-56

To search for text: 7-58
To repeat a search for text: 7-59
To search the capture buffer for a pattern: 7-60
To repeat a search for a pattern: 7-60
To jump to the marked frame: 7-60
To jump to the trigger frame: 7-60
To create a report: 7-62

Chapter 8. Managing Names and Working with Files

To edit the working name table: 8-7
To resolve unnamed stations by searching an external file: 8-9
To look for names within the frames in the capture buffer: 8-10
To automatically save the current working name table: 8-11
To manually save the current working name table: 8-11
To save frames in the capture buffer to a file: 8-12
To convert a trace file: 8-14
To load the capture buffer with a file of saved frames: 8-17
To delete a data file: 8-18
To save your current setup to the STARTUP file: 8-22
To save your current setup as a setup file: 8-23
To apply a saved setup file: 8-23
To restore Network General's default options: 8-23

Chapter 9. Using Protocol Forcing

To specify a protocol forcing rule: 9-4
To apply a protocol forcing rule: 9-11
To undo a forced protocol: 9-13

Chapter 10. Generating Traffic

To specify the destination of the generated frames: 10-5
To specify the size of the frames to be generated: 10-6
To specify the delay between generated frames: 10-6
To specify the number of frames to be generated: 10-7
To specify the contents of the data field: 10-8

To turn on the RI bit in the source address of a generated frame: 10-9
To generate traffic in buffer mode: 10-12
To start the Traffic generator: 10-13
To stop the Traffic generator: 10-14

Chapter 11. The Analyzer's File System

To configure Remote^2 Host to answer calls: 11-9
To create a new directory: 11-9
To specify the initial path to saved files: 11-10
To define the startup options: 11-12
To restore the factory defaults: 11-13
To create a name file from the current working name table: 11-14
To edit the startup parameters: 11-22

Chapter 12.Troubleshooting Guide

To access ngcgate via anonymous FTP: B-4
To access CompuServe: B-5
To access the Sniffnet BBS: B-5

Preface

Preface

About This Manual

This manual describes the functions and operations of the Expert Sniffer® analyzer, a software component of the Sniffer Network Analyzer. It also provides recommendations on how to use the analyzer effectively to detect and solve network problems.

The Sniffer Network Analyzer observes the local or wide area network to which it is attached, and displays the monitored activity.

Organization of This Manual

Figure i describes the organization of this manual.

Chapter/Appendix	Contents
Chapter 1, "Sniffer Network Analyzer Overview"	Provides an overview of the Sniffer Network Analyzer and describes its capabilities. Also defines key terms, lists new functions, and provides an introduction to the user interface.
Chapter 2, "Getting Familiar with the Expert Analyzer"	Provides an introduction to the Expert analyzer and describes fundamental Expert concepts. Also describes how to use user-defined Explain messages.
Chapter 3, "Defining System Options and Scheduled Events"	Describes global options that apply to all networks, as well as options for particular networks or platforms.
Chapter 4, "Defining Expert Analyzer Options"	Describes necessary pre-capture configuration for the Expert analyzer.
Chapter 5, "Navigating the Expert Window"	Describes how to move around in the various Expert analyzer displays and interpret the information presented within them.
Chapter 6, "Capturing Frames"	Describes how to prepare for capture, including setting capture filters, screen format options during capture, and a trigger to stop capture.

Figure i. Scope of each chapter and appendix

Chapter/Appendix	Contents
Chapter 7, "Displaying Interpreted Frames"	Describes the procedures for filtering, interpreting, displaying, and printing captured frames. Also provides general background information about protocol analysis.
Chapter 8, "Managing Names and Working With Files"	Describes the analyzer's name table and how to use data (trace) and setup files.
Chapter 9, "Using Protocol Forcing"	Describes the Protocol forcing function of the analyzer.
Chapter 10, "Generating Traffic"	Describes the traffic generator for Ethernet and token ring networks.
Chapter 11, "The Analyzer's File System"	Describes the network analyzer's directory structure and the types and formats of files it uses.
Appendix A, "Symptoms and Diagnoses"	Describes all symptoms and diagnoses generated by the Expert analyzer.
Appendix B, "Troubleshooting Guide"	Provides a list of solutions to common problems and procedures for contacting Technical Support.

Figure i. Scope of each chapter and appendix

Audience of This Manual

This manual assumes that:

- You are a network manager or troubleshooter who understands your network's operation.
- You are familiar with DOS.
- You have properly started the Sniffer Network Analyzer.

Navigational Aids Used in This Manual

To help you find procedures easily, a separate list of procedures is provided in this manual in addition to the Table of Contents and List of Figures.

This manual uses icons in the margin to help you locate information as explained below:

IMPORTANT: Next to this icon is information that is especially important; read it carefully before you proceed.

PROCEDURE. Next to this icon is a series of steps you must follow to accomplish a particular task.

Warning Box

WARNING. This box contains information you must know to avoid damage to data files, program files, or hardware devices.

Conventions Used in This Manual

Special Notations

The following describes the conventions used in this manual:

Bold	Menu options and menu names are in bold type. For example: Move to **Display** and press ENTER. Move to the **Report\Print** menu.
UPPERCASE	The filenames and command names you type at a DOS prompt are in uppercase. For example: Modify the AUTOEXEC.BAT file if necessary. To duplicate the file, use the COPY command.
Bold italics	Variables, for which you insert values, are in bold italics. For example: Type the number of minutes and seconds in the ***mm:ss*** format.
`Screen font`	Screen messages are printed in monospaced font. For example: `You must stop monitoring before you can use this feature.`

Terminology

Hexadecimal numbers mentioned in the manual are followed by "(hex)"; numbers without any notations are decimal. For example, "The maximum number of stations is 75. The default memory address is D8000 (hex)."

The term "application" refers to a software component (that is, the monitor or analysis program) running on the Sniffer Network Analyzer.

This manual sometimes uses abbreviated names for the various components of the Sniffer Network Analyzer. The term "analyzer" refers to the analysis application. The term "Expert analyzer" refers to the analyzer capturing or displaying in the Expert window.

Screen Displays

The screen displays in this manual may not exactly match what you see on your screen. There may be minor differences that do not affect the functions of the displays.

Other Sources of Information

Network General provides other sources of information to help you become familiar with the Sniffer Network Analyzer.

Manuals for the Sniffer Network Analyzer

Figure ii lists the manuals that accompany the Sniffer Network Analyzer. These manuals describe normal operations.

If the product shipment includes release notes or README files on disks, the information in the notes or files supersedes the information in this manual.

For Information On....	Read...
Installing and configuring the Sniffer Network Analyzer.	*Building the Sniffer Network Analyzer*
Operating the Sniffer analyzer in both Expert and Classic modes. General information on the Sniffer Network Analyzer.	*Expert Sniffer Network Analyzer Operations* (this manual)

Figure ii. Manuals for the Sniffer Network Analyzer

For Information On....	Read...
Accelerated overview of Expert analyzer operations. For those who don't like to read documentation.	*Expert Analysis Application Quickstart*
Operating the monitor functions on an Ethernet network. Using the monitor features effectively to detect network abnormalities.	*Sniffer Network Analyzer: Ethernet Monitor Operations*
Operating the monitor functions on a token ring network. Using the monitor features effectively to detect network abnormalities.	*Sniffer Network Analyzer: Token Ring Monitor Operations*
Operating the monitor functions on an FDDI network. Using the monitor features effectively to detect network abnormalities.	*Sniffer Network Analyzer: FDDI Monitor Operations*
Various network and protocol types.	*Network and Protocol Reference*
Remote^2 Manager.	*Sniffer Network Analyzer: DCA Remote^2 Supplement*

Figure ii. Manuals for the Sniffer Network Analyzer

Online Help

When you highlight an item in the analyzer or monitor menu, a phrase or sentence in a panel near the bottom of the screen explains the meaning of the highlighted item.

For general help information about a particular feature of the Sniffer Network Analyzer, press F1 **[Help]** at any time within the menus of the analysis or monitoring applications. A window containing a list of topics opens. These topics provide general descriptions and instructions for the items in the analyzer's menus.

In a monitor statistics screen, press F1 to get information about that screen.

In the Expert window, the key label for F1 reads **Explain**. Explain screens provide context-sensitive solutions to specific network problems highlighted in the Expert window.

Technical Support

If you have problems with the Sniffer Network Analyzer, refer to the troubleshooting section of this manual (Appendix B) for the procedure to contact Network General's Technical Support.

Figure iii shows Network General's Technical Support contact numbers.

Network General's Technical Support Department	
Toll-Free Telephone Number	(800) 395-3151
FAX Number	(415) 327-9436
FAX-on-Demand	(800) 764-3329
Internet Address	support@ngc.com
SniffNet BBS (2400 baud)	(415)-327-3875
SniffNet BBS (9600 baud)	(415)-327-4782
Compuserve	GO NETGENERAL
FAX on Demand	(800) 764-3329

Figure iii. Technical support contact information

Training

Network General offers a comprehensive set of training courses focused on hands-on network analysis and troubleshooting using the Sniffer Network Analyzer. For more information about these courses, contact your sales representative or call Network General Corporation.

Sniffer Network Analyzer Overview

1

Sniffer Network Analyzer Overview

Overview

This chapter provides a general orientation to the Sniffer Network Analyzer. The chapter summarizes the main features of the analyzer, provides a functional overview of the analyzer, and describes how to move around in the analyzer's menus. This chapter does not cover the procedures for invoking various Sniffer functions or explain in detail the various menu items. That information is provided in later chapters.

Major Components of the Sniffer Network Analyzer

The Sniffer analyzer is one of the software components of the Sniffer Network Analyzer. Figure 1–1 summarizes these major components.

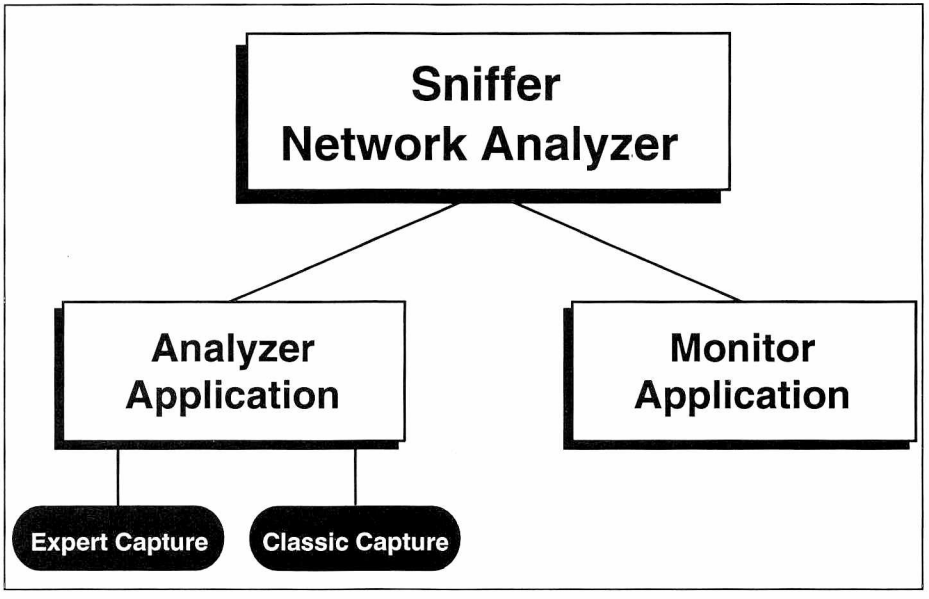


Figure 1–1. Major software components of the Sniffer Network Analyzer

Depending on the network topologies installed in your Sniffer Network Analyzer, you can capture in either Expert or Classic mode. Expert functionality is available on the following topologies:

- Ethernet
- Token ring
- WAN/Synchronous (the Expert Sniffer Internetwork Analyzer)

When this manual mentions the "Expert Sniffer analyzer," it is referring to the Sniffer analyzer capturing or displaying in Expert mode. Similarly, the term, "Classic Sniffer analyzer," refers to the Sniffer analyzer capturing or displaying in Classic mode.

Chapters 4 and 5 of this manual concentrate on capturing and displaying data with the Expert analyzer. Chapters 6 and 7 focus on capturing and displaying data with the Classic analyzer (standard traffic capture and protocol decodes).

Conceptual Overview of Sniffer Analyzer Functions

An analyzer —that is, the network analyzer program installed in the Sniffer Network Analyzer — records and interprets network transmissions. The work of the analyzer occurs in two main stages:

Capture

The analyzer records network traffic for up to 20 days for later interpretation. Capture can be filtered to record only traffic that meets certain criteria. Network data can be saved to disk when a user-definable trigger event occurs. This assures that the frames of interest are saved without requiring that capture be stopped. Alternatively, triggers can be specified so that capture stops when the trigger event is detected.

During capture in Expert mode, frames are analyzed as they are stored in the buffer. The various Expert displays are dynamically updated as capture proceeds, allowing you to navigate between various levels of detail to solve network problems in real time.

While capturing frames, the analyzer software maintains and displays graphs or tables that summarize recorded traffic.[1]

1. The analyzer's displays during capture resemble some of the displays produced by the monitor. Do not confuse this mini-monitoring during capture with the full-blown monitor application, which is separate.

Display

The analyzer interprets the recorded traffic. In the Classic window, the analyzer decodes the various layers of protocol in the recorded frames and displays them as English abbreviations or summaries. The analyzer can filter the display to show only those frames that meet certain criteria.

You can also display the captured frames in the Expert window. In the Expert window, you can investigate the symptoms and diagnoses the Expert analyzer detected. In the Expert window, all the views available during capture are also available during display. You can toggle display between the Classic and Expert windows by pressing the function key F3.

The Analyzer as (Mostly) Passive Observer

The Sniffer analyzer "hears" all traffic that passes over the segment it is observing. On a WAN/Synchronous link, it hears traffic in both directions ("from DTE" and "from DCE"). On a LAN, it hears all traffic that passes over the segment or subnet that it is monitoring. It is characteristic of a LAN that every station physically receives every transmission. Ordinarily, each station ignores all messages except broadcast messages and those addressed to it. The Sniffer analyzer not only hears all transmissions, but, while in "capture" mode, it can record them, no matter how they are addressed.

In general, the analyzer observes, tabulates, analyzes, or captures, but contributes no traffic to the network it is observing. However, when the analyzer is observing a LAN, it may contribute to the LAN's traffic:

- On Ethernet, token ring, FDDI, PCnet, ARCnet, and StarLAN, an analyzer can generate test frames. In this mode, it repeatedly transmits the single test packet you specify.
- On Ethernet, the analyzer can emit a pulse to test for cable defects.
- On token ring, every station must participate in the ring by forwarding traffic from its upstream neighbor to its downstream neighbor. The Sniffer analyzer does that in the same way as other stations. (The Token Ring 16/4 analyzer is an exception: it does not reply to the poll for standby monitors, and never acts as the ring's active monitor. It is thus invisible to most other stations.)

  NOTE: During traffic generation, the token ring analyzer may act as the active monitor if no other station is transmitting and responds to standby monitor polls.
- With most token ring adapters, the analyzer periodically transmits a frame addressed to "LAN Manager" announcing "trace tool present." The LAN Manager can force such a station to leave the ring immediately. The Token Ring-II analyzer, however does not support "trace tool present".

- On FDDI, the analyzer participates in the ring when it is set to SMT Active mode and forwards traffic from its upstream neighbor to its downstream neighbor. When set to SMT Passive mode, the analyzer forwards traffic but will not appear in an SMT ring map. When set up as a beam splitter, the analyzer is completely passive and doesn't affect the ring in any way.

A Map of the Analyzer's Functions

The analyzer's activities are divided into the set of functions described below. The diagram in Figure 1–2 represents schematically the route by which information flows between the various functions. Following the path of the frames as they are captured, they are affected by the analyzer's principal functions as follows:

- Capture filters determine which frames are discarded and which are captured.
- Capture views show the capture's progress, in one of two tabular formats or in the skyline format.
- Trigger detector scans arriving frames for a user-defined pattern or event. When it detects this pattern or event, it stops capture so that frames preceding or following the event are retained. Alternatively, you can configure **Disk Snapshot** so that the frames preceding or following the trigger event are saved to disk. This way, capture need not be stopped.
- Capture buffer is the storage area for frames that have been accepted. From here they are subsequently interpreted and displayed.
- Object database is the storage area for Expert information, such as network objects, symptoms, and diagnoses.
- Protocol interpreters identify the protocols nested within each frame and interpret their contents.
- Display filters determine which frames in the capture buffer are displayed.
- Frames that pass the display filters are displayed in three views:
  - — Summary
  - — Detail
  - — Hex with ASCII or EBCDIC

Output of the display can be saved to a file, sent to a printer, or imported into spreadsheets.

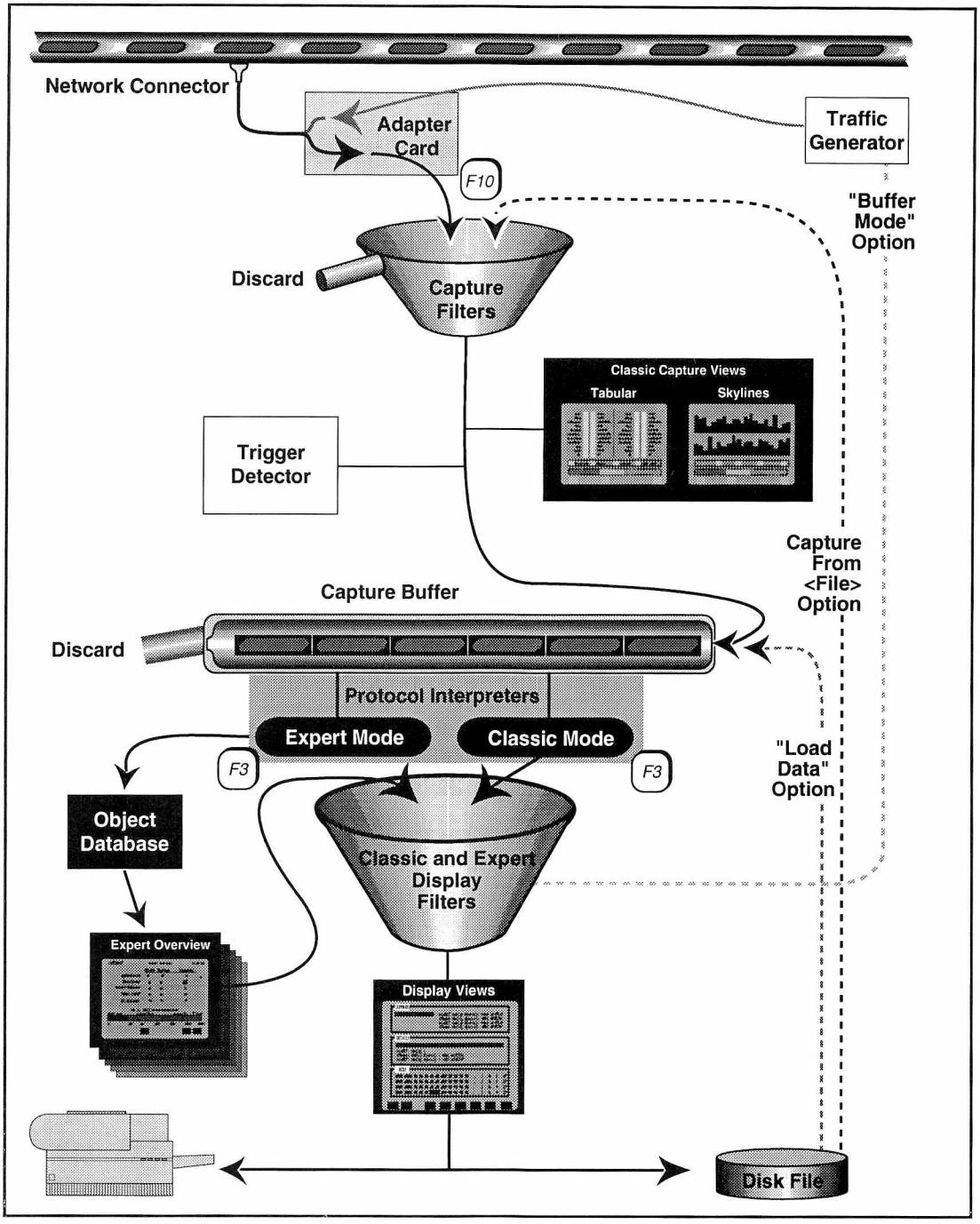


Figure 1–2. Overview of Sniffer analyzer functions

Starting the Sniffer Analyzer

This section describes how to start the Sniffer Network Analyzer as a whole and how to start the analyzer application specifically.

To start the Sniffer analyzer:

1. Power on the Sniffer Network Analyzer.

   Result: The Main Selection Menu of the Sniffer Network Analyzer appears. Figure 1–3 is similar but may not be identical to the Main Selection Menu on your network analyzer. The screens shown in this example are from an Ethernet analyzer. However, the procedure is the same for any other network type.

   NOTE: The Main Selection Menu includes a **Return to DOS** option. If you at any time exit to DOS, you can return to this Main Selection Menu by entering MENU at the DOS prompt.

2. If you want to enable the **Automatic Restart** option, use the cursor keys to highlight **Enable Automatic Restart** and press ENTER.

   Result: The Main Selection Menu reappears. The **Automatic Restart** option has changed to **Disable Automatic Restart**. (For more information about the **Automatic Restart** option, see "Automatic Restart Option" on page 11–21.

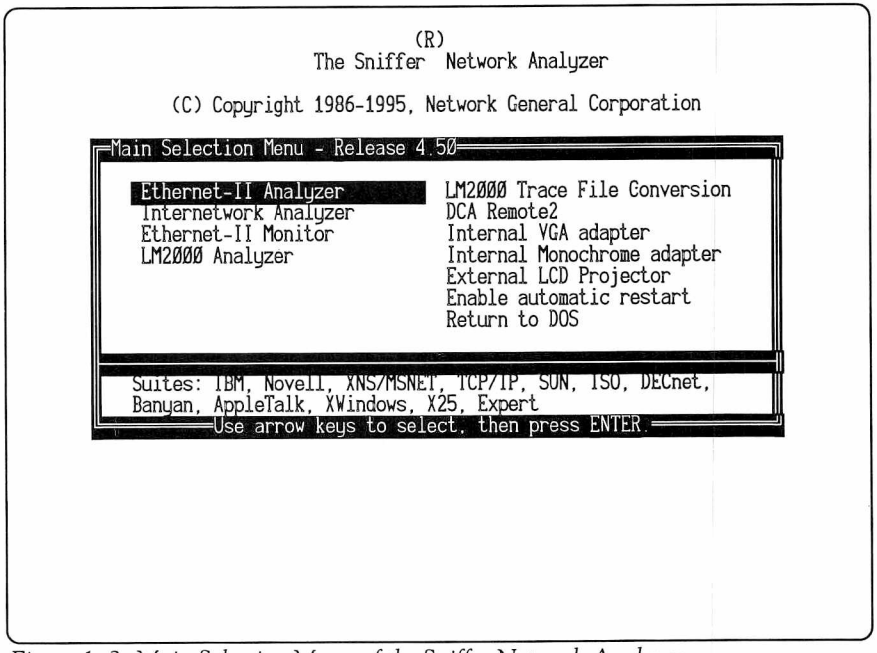


Figure 1–3. Main Selection Menu of the Sniffer Network Analyzer

3. Using the cursor keys, highlight the **Analyzer** menu option, and press ENTER.

Result: The Sniffer analyzer application is loaded into RAM. When initialization completes, the system will display a screen similar to Figure 1–4.

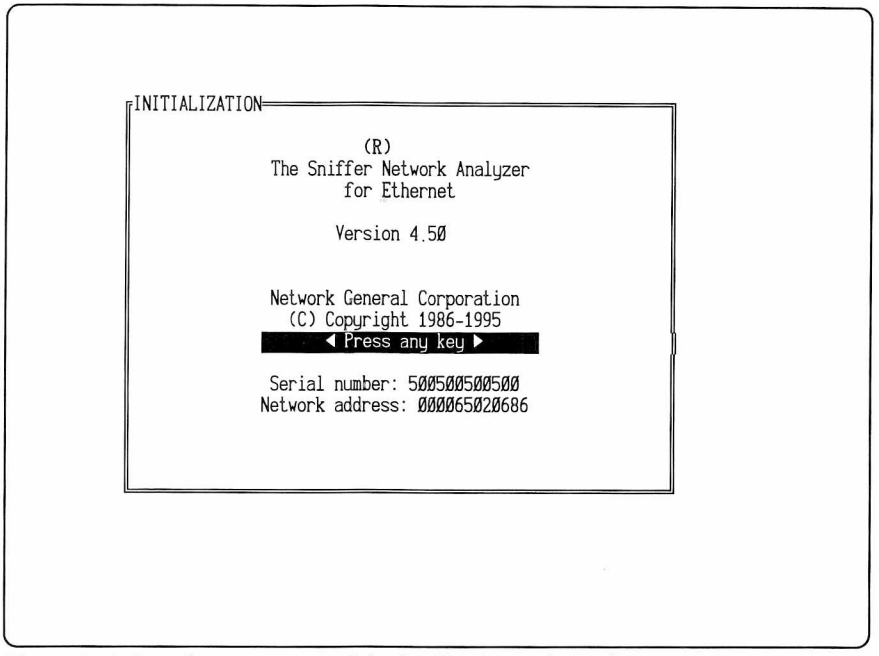


Figure 1–4. Initialization screen of the Sniffer Network Analyzer

4. Press any key.

   Result: The Main Menu of the Sniffer analyzer appears. From this menu you can control all Classic and Expert analyzer functions. Figure 1–5 shows the Main Menu of the Sniffer analyzer.

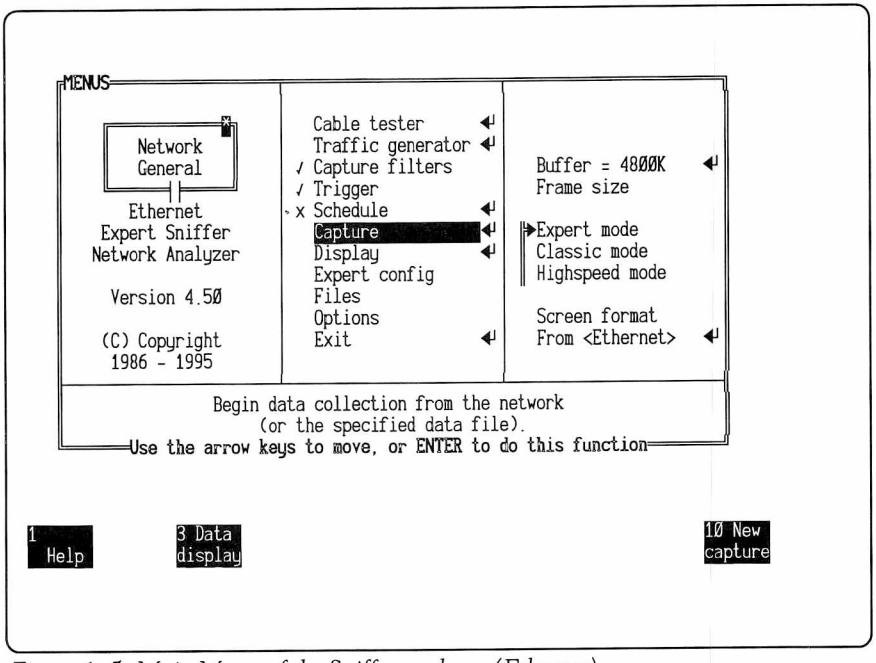


Figure 1–5. Main Menu of the Sniffer analyzer (Ethernet)

New Features of the Expert Analyzer

Figure 1–6 lists some of the new analyzer features in version 4.5.

Improved navigation in Frame Detail Display	You can now maintain the display at the same protocol layer when you display different frames.
Manufacturers' IDs	You can now choose whether or not the analyzer will translate the manufacturers' IDs in DLC addresses.
Automatic Restart	You can now configure the analyzer and monitor to restart a capture session when power is restored after a power failure. (This new feature is not available for the Notebook Sniffer Analyzer.)
Enhancements to Expert Analysis	Release 4.5 provides new expert analysis for NetWare 4.0 and for Banyan VINES version 5.5.
Enhancements to Classic Protocol Interpreters	Release 4.5 provides new or improved protocol interpreters for Novell NetWare 4.0, Banyan VINES version 5.5, SNMP-v.2, DLSw, LAPD (via a protocol forcing rule), Frame Relay, and PPP.
SIA Support for IBM Dock I	You can now use an IBM 750 or 755 notebook computer equipped with an IBM Dock I, Sniffer Internetwork Adapter, and Ethernet-III or Token Ring-III PCMCIA adapter.
Greenwich Mean Time	You can now save scheduled events in Greenwich Mean Time (GMT) instead of local time.
New Startup Parameters File	Startup parameters are now saved in the file \xxSNIFF\xxPARAM.BAT instead of in \xxSNIFF\xxSNIFF.MNU.
Improved Name Table	The name table is now stored in expanded memory, so you can set the maximum number of names (MAXSTNS) to any value up to 8000 without taking up space in conventional memory or in the Expert object space.
New Token Ring-II Adapter	The Token Ring-II analyzer uses a new and improved 16/4 Ringnode Plus adapter.
Force Open Option for Token Ring-II Analyzer	You can now configure the Token Ring-II analyzer to enter a beaconing ring.
Simplified Notebook Sniffer Analyzer Installation	The notebook Sniffer Network Analyzer installation process is now faster and easier. It also supports color or monochrome monitors.

Figure 1–6. New features of the Expert Sniffer analyzer

Overview of the User Interface

You interact with the analyzer through its menus and function keys. In some cases, a menu item and a function key have the same function. For example, you can either choose **Capture** from the main menu or press F10 **[New capture]** to start the capture process.

Using the Function Keys

In most cases, however, function keys are specific to whatever is displayed. During capture, for example, only those function keys that you might need are displayed. In Figure 1–7, F4 **[Clear screen]** clears the screen (although the capture buffer is not affected), F9 **[Pause]** pauses capture and displays additional function keys for additional options, and F10 **[New capture]** starts the capture. The function keys for various procedures are discussed with those procedures.

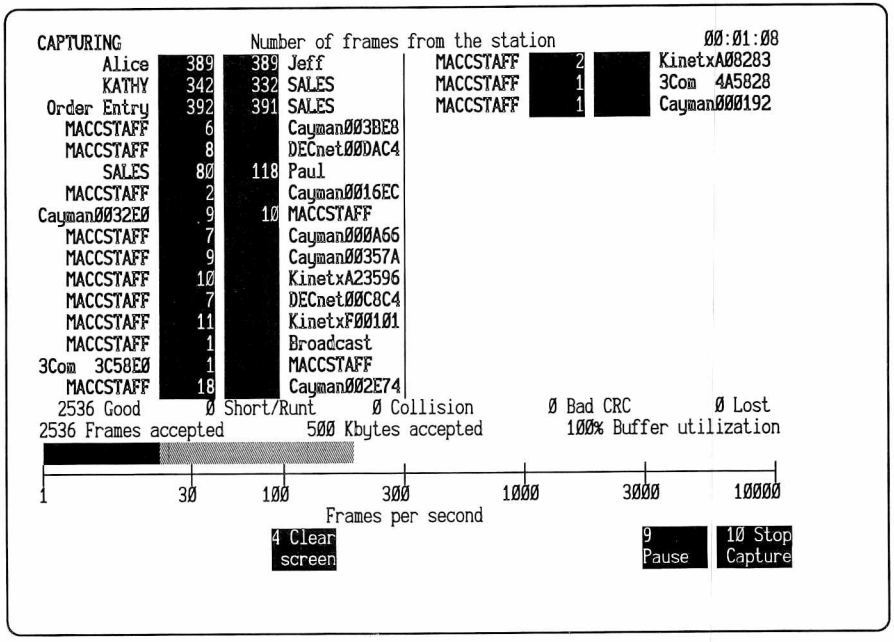


Figure 1–7. Function keys available during capture

Tree-Structure of the Analyzer's Menus

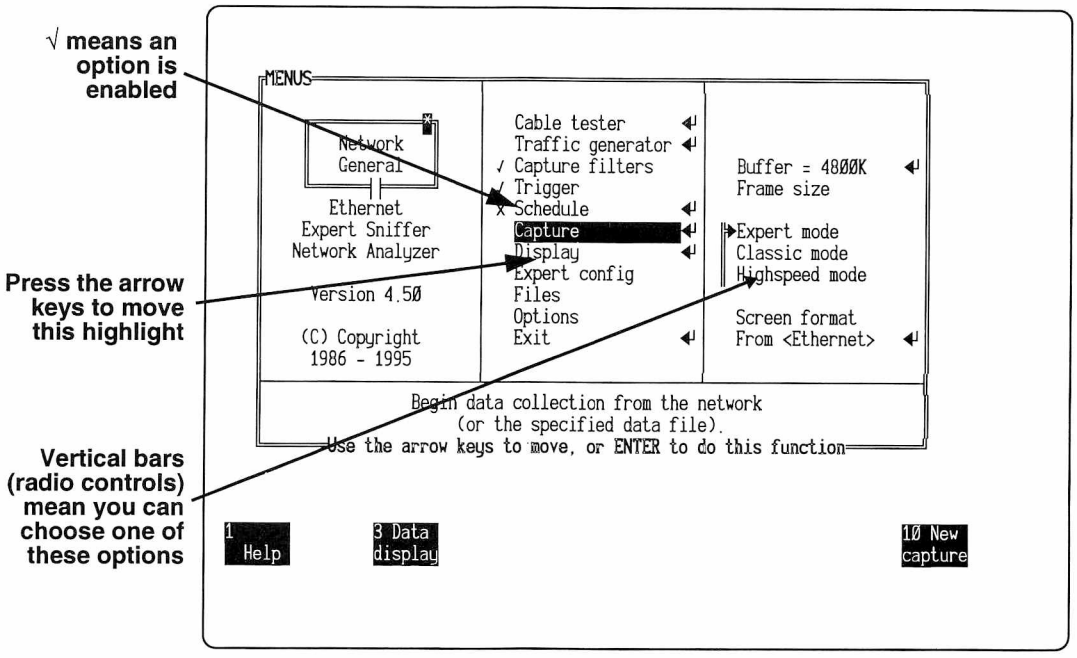


Figure 1–8. Main menu of the Sniffer analyzer (in this case, for Ethernet)

All Sniffer analyzer menus have the same structure. While details vary according to the network and protocol interpreter suites installed, the organization is the same. The entire menu is a tree, with its root (the main menu) to the left and its branches to the right. Only a part of the menu is visible at a time. Using the cursor keys, you move a window over the menu. Since the window is fixed on the screen, the menu appears to move under the stationary window.

When the menu is active, the screen shows three panels. You control the center panel. Within that center panel, the center row is highlighted. That is your location on the menu. When you first start the analyzer, the center panel lists the alternatives available from the root of the tree.

When you press the CURSOR UP key, the item above Capture becomes highlighted. We speak of "moving the highlight up" to the next item. The highlight doesn't really move; instead, the entire center panel scrolls downward so that the (stationary) highlight is now on the row above. Alternatively, to jump directly up or down to a particular item, type the first letter of its name. The highlight jumps to the next item beginning with that letter.

The right panel shows submenus for the highlighted item in the center panel. When you highlight a different item, the right panel changes to show the submenu that goes with the highlighted item.

To work with the Sniffer analyzer menus:

1. Press one of the four arrow keys to move the highlight to the desired menu item. Any options associated with that item appear in the panel to the item's right. As you move the highlight, the relevant options are displayed, while those associated with another option disappear.
2. For options followed by a ↵ symbol, pressing ENTER when the option is highlighted either executes the command or it displays a listing or dialog box. From this display, you can either choose an option or enter information. In Figure 1–8, for example, pressing ENTER when the **From <Ethernet>** option is highlighted results in a listing of files from which you can choose one as the capture source.
3. For options connected by a vertical bar (radio control), you can choose an option by moving the highlight to that option and pressing Spacebar. All other options connected by the bar are automatically disabled. In the main menu, for example, you can choose between capturing in **Expert mode** or in **Classic mode**.
4. For options preceded by √ or x symbols, you can enable or disable those options by moving the highlight to them and pressing Spacebar. Any such options are always either enabled (√) or disabled (x); pressing Spacebar toggles between the two states.

To use online help:

1. Press F1 **[Help]** to display the **Help** menu or relevant submenu. If you press F1 when one of the monitor views is displayed, a description of that view appears.
2. In a **Help** menu, move to the topic for which you want additional information and press ENTER.

   To scroll through help text, press CURSOR UP, CURSOR DOWN, PAGE UP, or PAGE DOWN.
3. Press ESC to return to the **Help** menu. Press ESC again to return to the screen displayed before you used online help.

Using a Mouse with the Analyzer

The analyzer supports a standard two-button mouse as a supplement to keyboard operation. You must install your own mouse and its corresponding mouse driver. Follow the mouse manufacturer's instructions. If you want the mouse to be available

whenever you use the analyzer, then put a suitable mouse command in your CONFIG.SYS or AUTOEXEC.BAT file.

The mouse appears as a rectangular cursor on the screen. Press the mouse's left button to select the item at the mouse cursor's location. If the item is already highlighted, then pressing the left button is like pressing ENTER. Pressing the mouse's right button is like pressing the ESC key.

The best way to learn to use the mouse is by simple experiment. Most of the operations are intuitive. However, there are some things that it might not occur to you to try. Therefore, the following table summarizes the operations you can perform with the mouse.

Category	Mouse Operation	Equivalent keyboard function/Description
General	Left click on a function key.	Presses the function key.
	Left click on a highlighted item.	Presses ENTER.
	Right click.	Presses ESC.
Menu Tree	Left click on an item.	Makes it the center item in the display.
	Left click on a highlighted item.	Presses ENTER or the Spacebar (enable/disable), as appropriate for that item. If an item allows both functions, clicking on the ↵ symbol presses ENTER.
	Left click on the top or bottom edge of the center column	Presses PAGE UP or PAGE DOWN.
List Windows	Left click on the top or bottom edge.	Presses PAGE UP or PAGE DOWN.
	Left click on an item.	Highlights that item.
	Left click on a highlighted item.	Selects it, such as pressing ENTER.
Summary/ Detail/ Hex Windows	Left or right click on the left or right edge.	Scrolls down or up.
	Left or right click on the bottom edge, but not in the "Frame x of y" area.	Scrolls left or right.
	Left or right click on the bottom edge, in the "Frame x of y" area.	Displays the "go to frame number" dialog box.
	Left or right click on the top edge.	Presses PAGE UP or PAGE DOWN.
	Left click inside a display window.	Makes that display window the focus.
	Left double-click inside a display window.	Zooms in and out.
	Left click in a different display window.	Makes that display window the active window.
Expert Display	Left click on the top or bottom edge of the Summary screen.	Presses PAGE UP or PAGE DOWN.
	Left click on the top or bottom edge of the Detail screen.	Scrolls up and down in the list of objects.
	Left click on the top or bottom edge of the Statistics screen.	Scrolls up and down in the list of objects.

Figure 1–9. Mouse functions

Getting Familiar with the Expert Analyzer

2

Getting Familiar with the Expert Analyzer

Overview

This chapter defines key Expert analyzer concepts, tells how to start the analyzer in Expert mode, and describes how to navigate among the Expert analyzer screen displays. The chapter gives you a "feel" for how the Expert analyzer operates, but does not discuss in detail the various features of the analyzer. The screens in this chapter are samples that illustrate the effects of various steps; you might see different messages on your analyzer as you follow the instructions.

Sniffer analyzers (except the FDDI Sniffer Analyzer) can capture in either Expert or Classic mode. The manual will sometimes refer to the ***Expert analyzer***. When it does, it means the Sniffer analyzer capturing or displaying in Expert mode.

This chapter assumes that you have successfully started your Sniffer Network Analyzer, attached it to the network, and displayed the Main Selection Menu. If you have not done so, refer to the *Building the Sniffer Network Analyzer* manual to learn how to get started with the Sniffer Network Analyzer.

Expert Analyzer Terminology

When you start capture in Expert mode, the analyzer immediately begins constructing a database of *network objects* from the traffic it sees. The Expert analyzer uses its real-time protocol interpreters to learn about all the network stations, routing nodes, subnetworks, and connections related to the frames in the capture buffer. Using this information, the Expert analyzer can detect and alert you to potential problems that may be plaguing the network. The analyzer categorizes network problems as being either *symptoms* or *diagnoses*. The next section defines network objects, symptoms, and diagnoses.

About Network Objects

The amount of raw data on a network can be quite large. By performing multilevel protocol analysis on the frames that pass through its real-time protocol interpreters, the Expert analyzer extracts a small number of network objects from the huge amount of information it processes.

Network objects can be any of the following:

- A DLC station
- A network station
- A connection
- An application
- A subnetwork

The Expert analyzer learns about a network by correlating the various network objects it creates.

About Symptoms

When the analyzer detects an abnormal or unusual network event, it considers such an event a "symptom" that indicates a possible network problem. The analyzer displays a symptom message in an Expert window.

After establishing an accurate network baseline, you can alter the Expert thresholds to modify symptoms. That is, you can specify that a certain network parameter (for example, the number of identical requests sent by an application) must exceed a certain limit before the analyzer displays a symptom message. (For information on setting thresholds, see "Setting Thresholds for Symptoms and Diagnoses" on page 4–13.)

About Diagnoses

In addition to revealing symptoms, the analyzer generates "diagnoses." There are two types of diagnoses:

- A diagnosis caused by several symptoms or recurrences of a symptom. As a symptom becomes more severe, the analyzer concludes that the symptom is not only an indicator but also a problem in itself.

  For example, if network traffic increases suddenly over a short period of time, the Expert analyzer may alert you to a **LAN overload** symptom. If the **LAN overload** symptom persists over a longer period of time, the analyzer will display a **LAN overload** diagnosis. You can define thresholds for this type of diagnosis. For example, you could specify that a **LAN overload** diagnosis be generated whenever a **LAN overload** symptom is active for more than 20 percent of a minute.

- A diagnosis caused by a single network event that is itself considered to be problematic. The analyzer immediately assumes that the event represents a problem; these kinds of diagnoses have no user-defined thresholds.

For example, when the Expert analyzer detects two stations with the same network address, it will immediately display the symptom and diagnosis **Duplicate network address**. This diagnosis has no threshold to exceed.

The Expert analyzer uncovers symptoms and provides diagnoses. You draw a conclusion based on the information gathered by the analyzer and your knowledge of the network.

Capturing and Analyzing Frames in Expert Mode

Network General provides the Expert Sniffer Analyzer application with a set of default Expert thresholds that determines under what conditions the Expert analyzer will indicate various network problems. These default settings make the Expert analyzer a turnkey application requiring little or no configuration.

This section describes how to start the Expert analyzer capturing with the default settings. There are other ways to run the Expert analyzer; the following procedure is just one of them. Chapters 4–5 describe how to customize an Expert capture session. Chapter 6 describes how to customize a Classic capture session.

When you start the Sniffer analyzer from the Main Selection Menu, it automatically defaults to Expert capture mode. Note that the pointer in the far right panel of Figure 2–1 points to **Expert mode** rather than **Classic**.

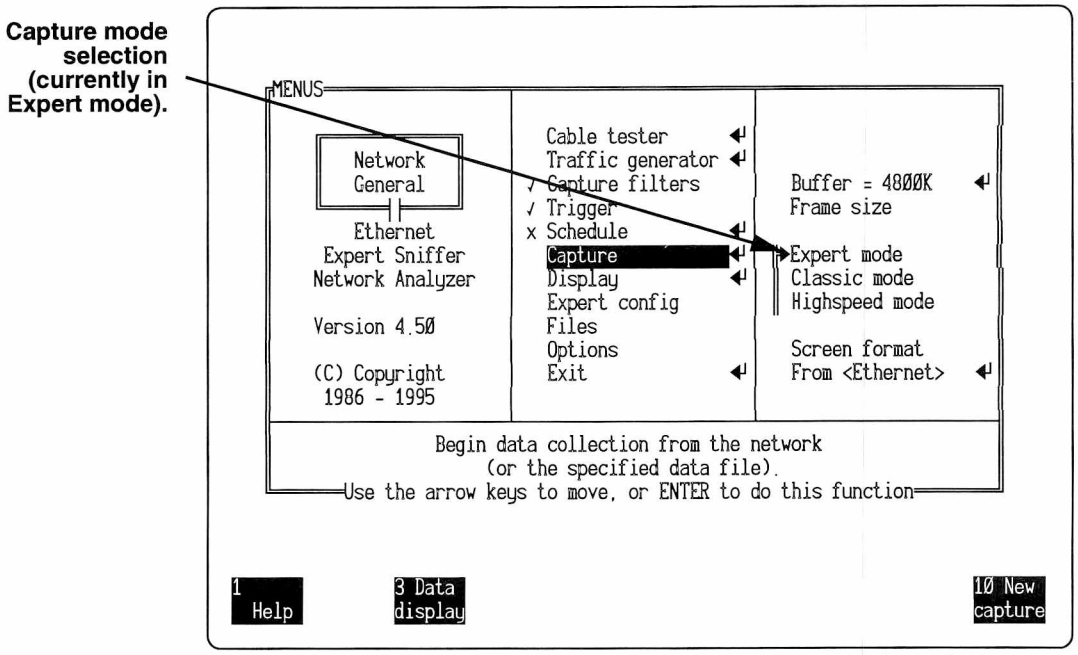


Figure 2–1. Main Menu of the Sniffer analyzer (in this case, for Ethernet)

Press F10 **[New Capture]** to start capture. Alternatively, you can use the cursor keys to highlight **Capture** and press ENTER.

Result: The analyzer begins capturing in Expert mode. The Expert Overview appears (Figure 2–2), displaying the results of Expert analysis as it captures frames.

Diagnosis count column. Notice that the analyzer has already made three diagnoses at the Expert Application layer.

Network object counters. The analyzer has detected 15 objects at the Expert Application layer. See page 2–3 for a definition of network objects.

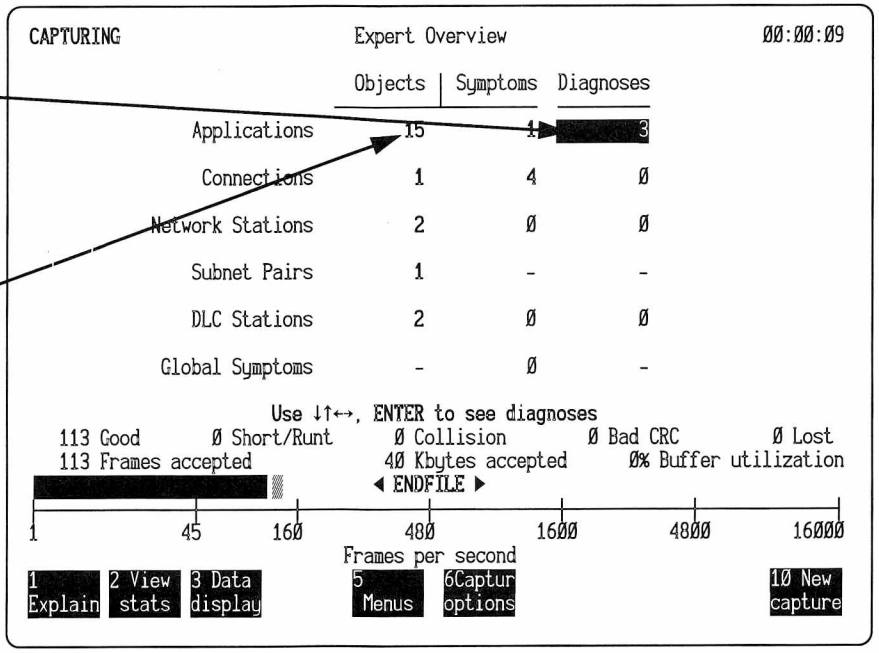

CAPTURING
Expert Overview
00:00:09
Objects | Symptoms | Diagnoses
Applications 15 1 3
Connections 1 4 0
Network Stations 2 0 0
Subnet Pairs 1 - -
DLC Stations 2 0 0
Global Symptoms - 0 -
Use ↓↑↔, ENTER to see diagnoses
113 Good 0 Short/Runt 0 Collision 0 Bad CRC 0 Lost
113 Frames accepted 40 Kbytes accepted 0% Buffer utilization
◀ ENDFILE ▶
1 45 160 480 1600 4800 16000
Frames per second
1 Explain
2 View stats
3 Data display
5 Menus
6Captur options
10 New capture

Figure 2–2. Expert Overview window of the Expert analyzer

Notice that in Figure 2–2 the Diagnoses column already indicates three diagnoses made at the Expert application layer. The Expert analyzer has uncovered problems on your network based on the symptoms and network objects it has detected. You can decide whether you want to see the diagnoses and further investigate the cause of these problems.

The analyzer categorizes network problems according to the Expert layer at which they occur. Expert layers have a rough parallel in the OSI model. For a complete description of how the Expert model of the network compares to the OSI model, refer to "Expert Layers and the OSI Model" on page 4–4.

About the Expert Window

Once capture in Expert mode begins, you are in the ***Expert window***. The term ***Expert window*** refers to the set of available Expert screen displays in which you can view the results of Expert analysis. In general, the following types of Expert screen displays are available in the Expert window.

- Overview
- Summary
- Detail
- Statistics

These screens vary depending on many factors; this chapter describes several. For a complete description of all displays available in the Expert window, refer to Chapter 5, "Expert Analyzer Capture and Display." Note that the Expert window is the same whether you are capturing frames or just displaying them.

Getting More Information About a Diagnosis

The Expert Overview shows the number of diagnoses per Expert layer but not the diagnoses themselves. You might want to view the list of diagnoses and elect to investigate one diagnosis at a time.

To obtain more information about a diagnosis:

1. In the Diagnoses column of the Expert Overview, use the cursor keys to highlight an Expert layer that has at least one diagnosis. Press ENTER.

   Result: A list of diagnoses at the selected Expert layer appears. Figure 2–3 is an example of the Diagnosis Summary screen at the Application layer.

   If no diagnoses have been detected at the highlighted layer, nothing will happen when you press ENTER. If there are diagnoses at the highlighted layer, the help line at the bottom of the capture display will change to read, "ENTER to see diagnoses."

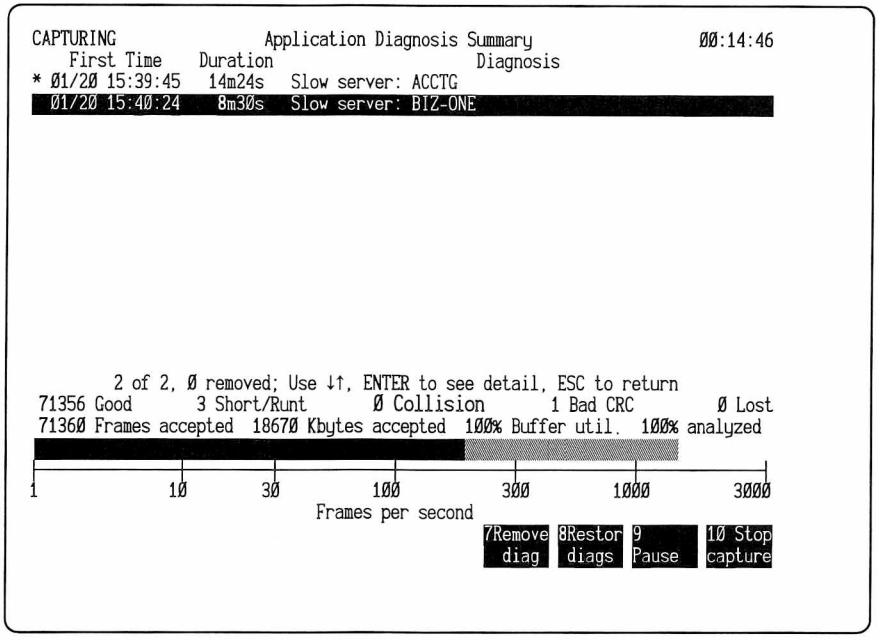


Figure 2–3. Application Diagnosis Summary window

2. You can obtain more detailed information on any diagnosis. Use the cursor keys to highlight a diagnosis and press ENTER to display a Diagnosis Detail screen, which contains further information regarding the selected diagnosis.

   For example, in Figure 2–3, the Diagnosis Summary view shows that the Expert analyzer has diagnosed the server BIZ-ONE as being slow. In Figure 2–4, the Diagnosis Detail screen shows which stations received a slow response from BIZ-ONE.

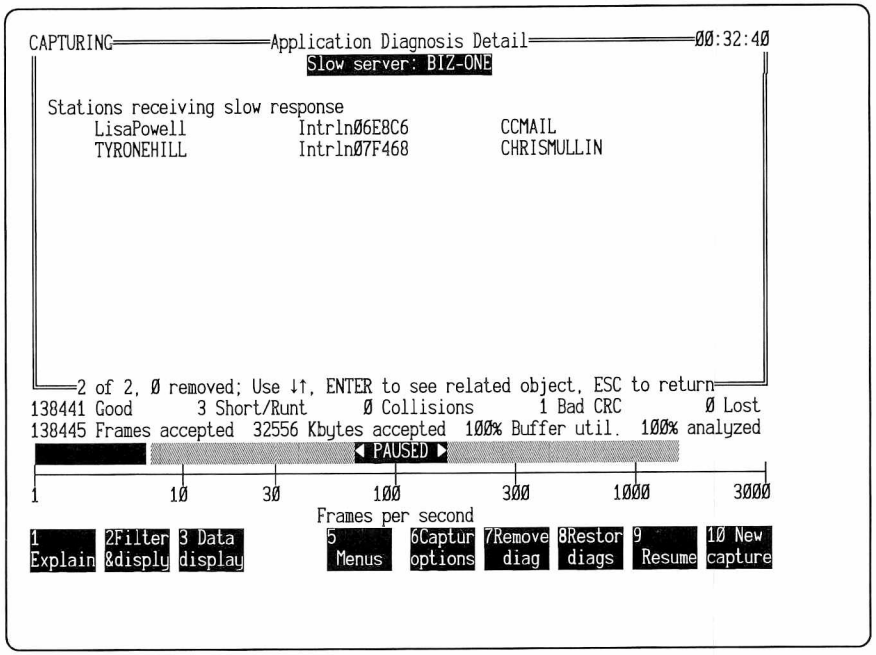


Figure 2–4. Application Diagnosis Detail screen

The Diagnosis Detail screen in Figure 2–4 shows which nodes received a slow response from the server BIZ-ONE; however, it does not describe the network conditions that led the analyzer to arrive at this diagnosis or how you might go about correcting the problem. To get more information about this diagnosis, you may want to invoke the Expert analyzer's Explain screen.

Getting Context-Sensitive Explain Messages

The Expert analyzer displays concise diagnostic and symptom windows. If you do not fully understand the nature of the problem indicated by an Expert detail or summary window, or would like the opinion of the Expert analyzer, invoke the context-sensitive Explain message. Such a message tells you why the analyzer "thinks" that a problem exists, what other areas you might want to examine to determine the seriousness of the problem, and what thresholds affect the current symptom or diagnosis.

Explain messages are always available in the Expert window, whether during capture (if paused) or during post-capture display routines. You can pause capture at any time and invoke an Explain message. Do not confuse Explain messages with help messages, which are invoked by the same function key.

The help messages serve as reminders about items in the analyzer's menus. Explain messages provide further information that is not in the current Expert view but may be important for your investigation of network problems. You can tell which type of message will appear by examining the dynamic function key labels at the bottom of the display. In Figure 2–4, F1 is labeled as **Explain**, and will display an Explain message when pressed, rather than a help message.

To display an Explain message during capture:

1. While in the Expert window, press F9 **[Pause]** to stop capture temporarily.
2. Press F1 **[Explain]**.

   Result: The Expert analyzer displays a context-sensitive Explain message related to the current Expert view or highlighted item.

During post-capture display, Explain messages are always available in the Expert window. Press F1 to see them.

Figure 2–5 shows the Explain message for the **Slow server** diagnosis from the previous example. Notice that the Application Diagnosis Detail view from Figure 2–4 is still visible behind the Explain screen.

```
CAPTURING═══════════Application Diagnosis Detail═══════════00:00:21
                    Slow server: BIZ-ONE

Stations receiving slow response
     AlexMorton          Intrln06E8C6        CCMAIL
     ChrisWebber         Intrln07F468        CHRISMULLIN

EXPERT EXPLAIN═══════════════════════════════════════════════════
  Diagnosis:  Slow server: BIZ-ONE

The ratio of slow responses to total responses for a particular station
has exceeded the "Slow resp %" threshold of 20 percent. A slow response
is one in which the time between request and response is longer than the
"Resp time" threshold of 100ms.


Possible cause:

This usually means that your server is overloaded. You should examine the
traffic to your server to see if the traffic is justified. If so, you
should consider getting a faster server or distributing the load across
multiple servers.
          More↓═══Use ↓↑ keys to move, or ESC to return.═══════════
```

Figure 2–5. Explain screen for the diagnosis ***Slow server***

Explain messages vary according to the context. For example, if the symptom message highlighted is `Many routers to remote network`, the Explain message shows you

specifically the connections among the network station and the routers. The network addresses and the configuration shown in the message can be different each time depending on the node and routers involved. Similarly, when you display a detail window for a diagnosis or symptom, the exact Explain message depends on the information in the detail window.

User Explain Messages

Overview

You can create your own context-sensitive explain messages and display them along with the corresponding Network General text in the Expert Explain windows.

If you don't want to add your own messages, do nothing. The Network General messages will be the only ones displayed. If you want the user explain feature, follow the directions in *"Setting Up User Explain,"* below.

Setting Up User Explain

Your analyzer software includes the following set of user explain template files:

\xxSNIFF\XPHELP\XPUSER.US*.TPL

where *xx* is the network adapter type — for example, EN for Ethernet.

To set up the user explain, copy these files to a new set with a .USR extension:

```
CD \xxSNIFF\XPHELP\XPUSER.US

COPY *.TPL *.USR
```

When you have copied the files, you will see empty templates displayed along with Network General's explain messages, as shown in Figure 2–6.

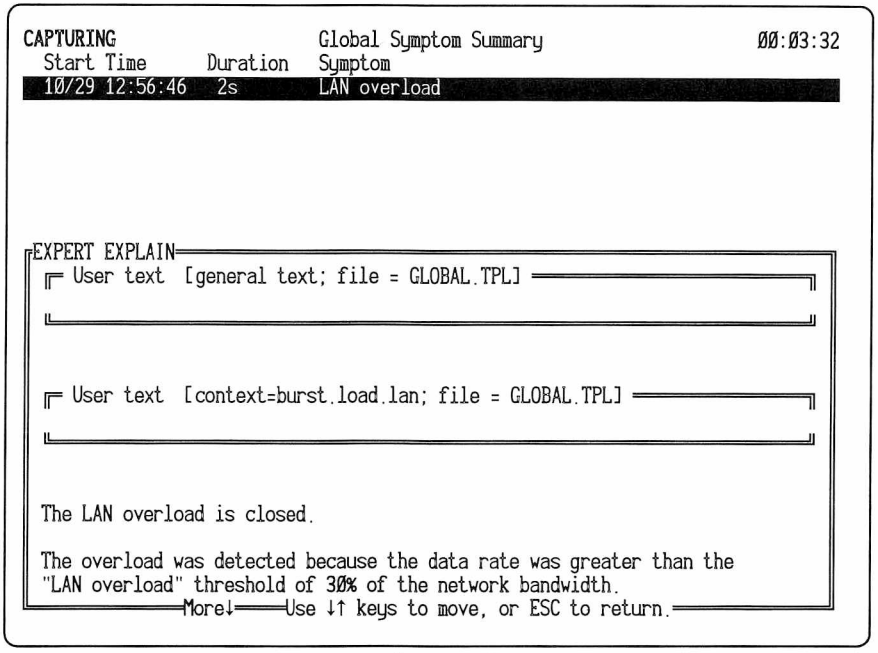


Figure 2–6. Context-sensitive user explain templates

Editing the User Explain Files

When you edit the user explain (.USR) files, use an ASCII text editor like the MS-DOS editor in Figure 2–7.

Do not use a single % sign when you enter text. The % sign is reserved for the special parameters passed to the Network General explain messages by the analyzer software. If you want to display a % sign, enter "%%".

Each of the context-sensitive template boxes shown in Figure 2–6 has a context id and a template (.TPL) filename. To add your own explain message, simply open the corresponding .USR file and type your message into the appropriate box, according to the context identification.

For example, suppose that you have been noticing a **LAN overload** symptom on your network at about 1 p.m. each day. You can add a special message to the user explain, as shown in the following screen:

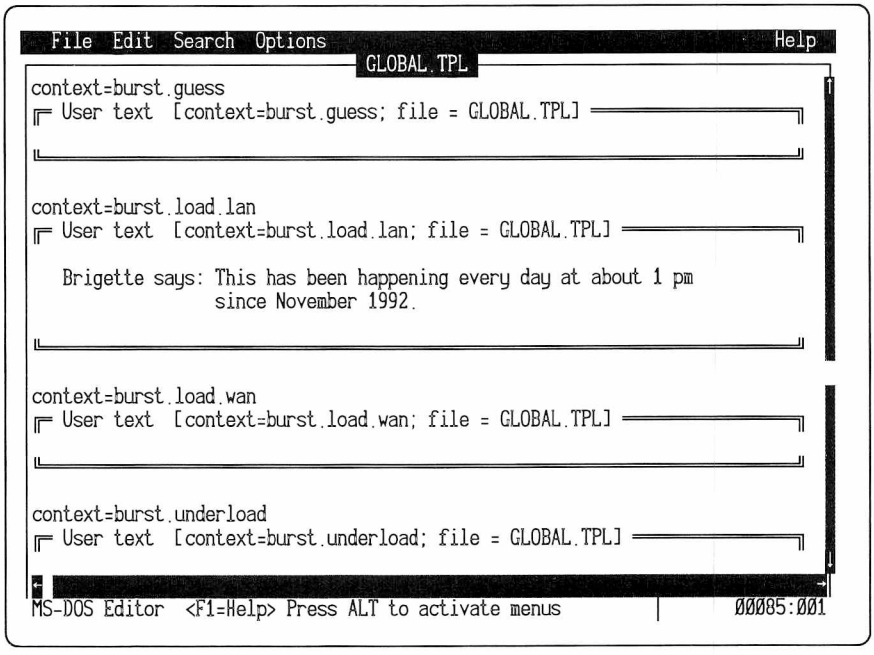

File Edit Search Options Help
GLOBAL.TPL
context=burst.guess
User text [context=burst.guess; file = GLOBAL.TPL]
context=burst.load.lan
User text [context=burst.load.lan; file = GLOBAL.TPL]
Brigette says: This has been happening every day at about 1 pm
since November 1992.
context=burst.load.wan
User text [context=burst.load.wan; file = GLOBAL.TPL]
context=burst.underload
User text [context=burst.underload; file = GLOBAL.TPL]
MS-DOS Editor <F1=Help> Press ALT to activate menus
00085:001

Figure 2–7. Adding a user explain message to the GLOBAL.TPL file

In addition to the context-sensitive explain messages, you can also add general text that will be displayed for a broader set of situations. For example, you can type a message into the general text box shown in Figure 2–7, and it will be displayed as an explain message for all **Global Symptoms** explain screens, or for all explain text in GLOBAL.TPL.

To make changes to the user explain, edit the .USR files. You can also create multiple sets of potential user explain files, with extensions that you choose — for example, .TP1, TP2. Then you can activate a particular set by copying or renaming it to *.USR.

Displaying the User Explain Messages

To display the user explain messages, just make sure that each file you want to display has a .USR extension. Your explain message(s) will appear just above the corresponding Network General explain message(s) whenever the same situation (in this example a LAN overload) occurs. The end result will be as shown in Figure 2–8. If you have a color display, the user explain will appear in red, and the Network General explain will appear in black.

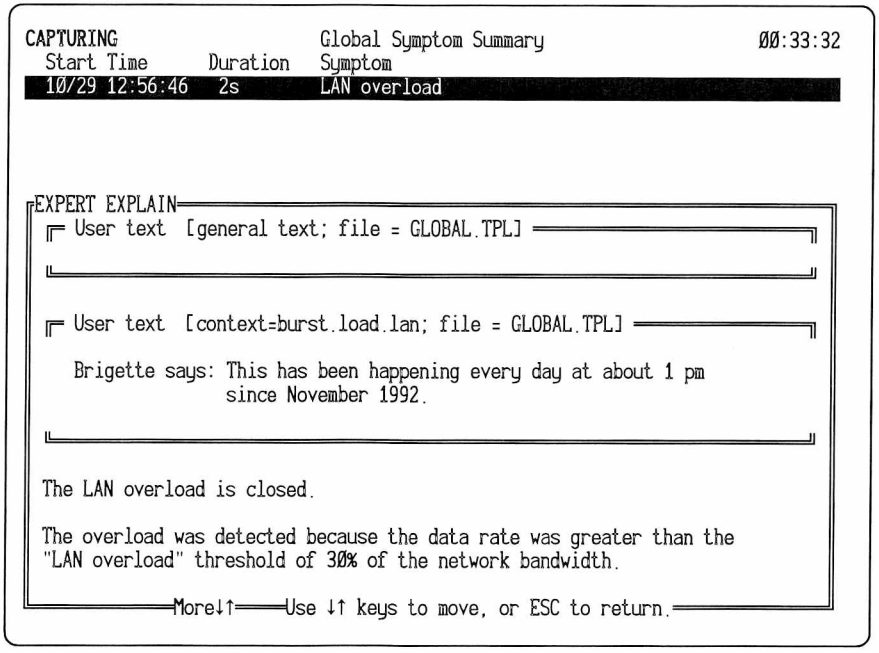

CAPTURING
Global Symptom Summary
ØØ:33:32
Start Time
Duration
Symptom
10/29 12:56:46
2s
LAN overload
EXPERT EXPLAIN
User text [general text; file = GLOBAL.TPL]
User text [context=burst.load.lan; file = GLOBAL.TPL]
Brigette says: This has been happening every day at about 1 pm
since November 1992.
The LAN overload is closed.
The overload was detected because the data rate was greater than the
"LAN overload" threshold of 3Ø% of the network bandwidth.
More↓↑
Use ↓↑ keys to move, or ESC to return.

Figure 2–8. User explain text for the LAN overload symptom

Getting More Information About Symptoms and Network Objects

You display the Expert analyzer's database of symptoms and network objects just as you would display information about diagnoses. From the Expert Overview, use the cursor keys to highlight the appropriate layer in the Objects/Symptoms column and press ENTER. Figure 2–9 shows the Expert Overview with the Objects/Symptoms column highlighted at the Connections layer.

When you move the highlight to the Objects/Symptoms column, the highlight automatically expands to cover both columns. This indicates that you cannot view objects without viewing symptoms, and vice-versa.

You cannot view network objects without viewing symptoms.

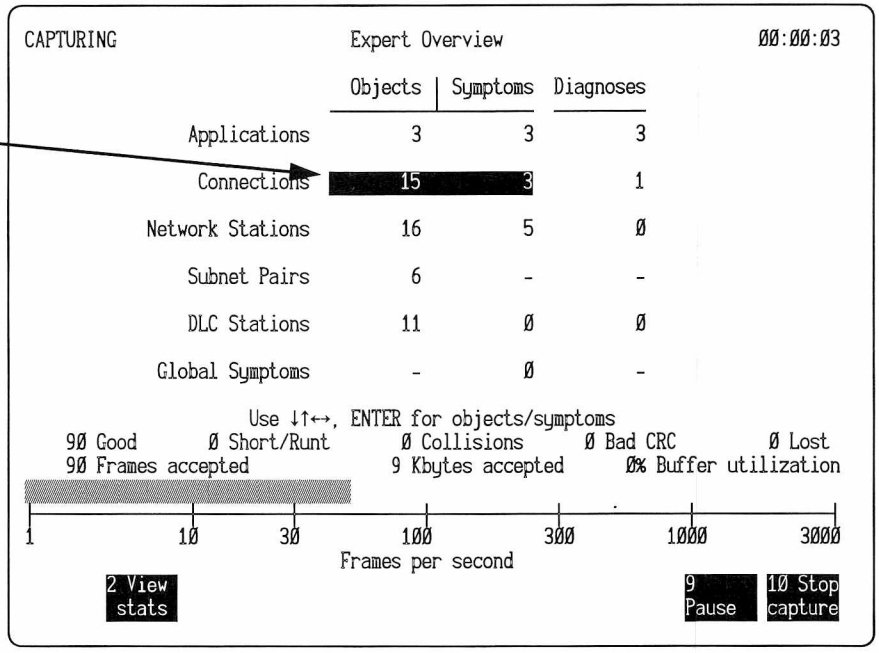


Figure 2–9. Expert Overview screen

A list of network objects detected at the selected Expert layer appears. The list includes a description of the last symptom (if any) associated with each network object. This list is called a Summary window. Figure 2–10 shows the Summary window at the Connection layer.

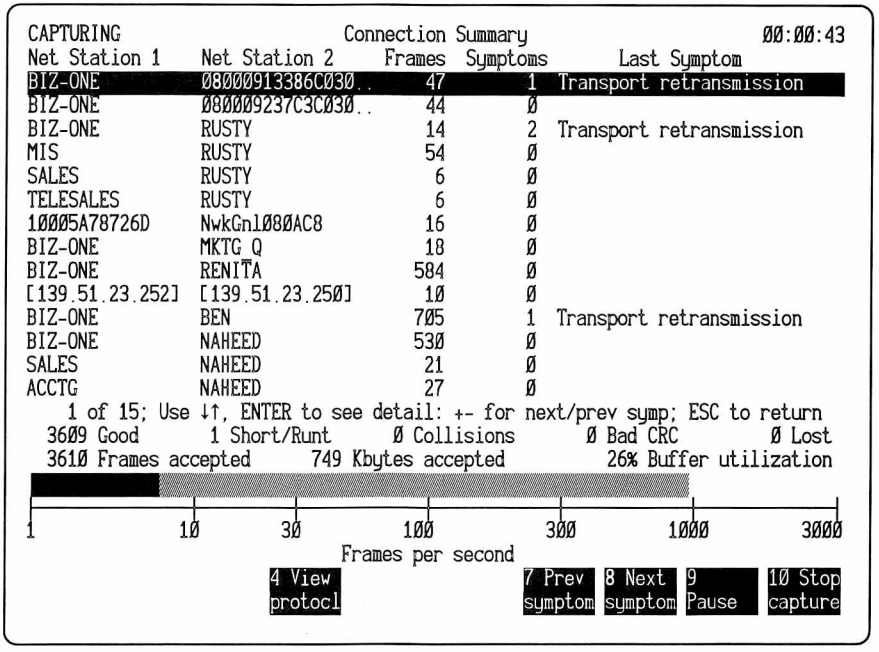
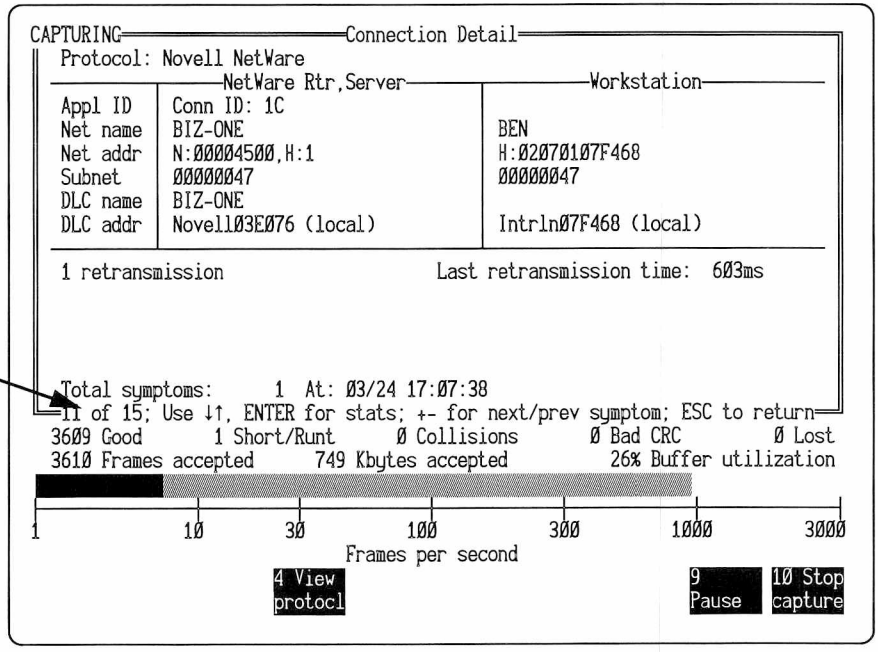

CAPTURING Connection Summary ØØ:ØØ:43
Net Station 1 Net Station 2 Frames Symptoms Last Symptom
BIZ-ONE Ø8ØØØ913386CØ3Ø.. 47 1 Transport retransmission
BIZ-ONE Ø8ØØØ9237C3CØ3Ø.. 44 Ø
BIZ-ONE RUSTY 14 2 Transport retransmission
MIS RUSTY 54 Ø
SALES RUSTY 6 Ø
TELESALES RUSTY 6 Ø
1ØØØ5A78726D NwkGnlØ8ØAC8 16 Ø
BIZ-ONE MKTG Q 18 Ø
BIZ-ONE RENITA 584 Ø
[139.51.23.252] [139.51.23.25Ø] 1Ø Ø
BIZ-ONE BEN 7Ø5 1 Transport retransmission
BIZ-ONE NAHEED 53Ø Ø
SALES NAHEED 21 Ø
ACCTG NAHEED 27 Ø
1 of 15; Use ↓↑, ENTER to see detail: +- for next/prev symp; ESC to return
36Ø9 Good 1 Short/Runt Ø Collisions Ø Bad CRC Ø Lost
361Ø Frames accepted 749 Kbytes accepted 26% Buffer utilization
1 1Ø 3Ø 1ØØ 3ØØ 1ØØØ 3ØØØ
Frames per second
4 View protocl
7 Prev symptom
8 Next symptom
9 Pause
1Ø Stop capture

Figure 2–10. Connection Summary window

To get detailed information about a particular connection or symptom, use the cursor keys to highlight a connection in the Summary window and press ENTER. A detailed display appears as shown in Figure 2–11. The Detail window provides information such as the network addresses of the two endpoints of a connection, the protocol used, and any symptoms associated with the particular connection, network station, or DLC station.



You can use the cursor keys to scroll through the Detail windows for any of the 15 connections detected by the analyzer.

Figure 2–11. Connection Detail window

Notice that at the bottom of the Connection Detail border in Figure 2–11, the display reads, "11 of 15." From the Detail window, you can use the cursor keys to page through the Detail windows for any of the 15 connections detected by the Expert analyzer. Alternatively, you can press ENTER again, and see a Statistics window for a particular connection, network station, or DLC station. Figure 2–12 shows a typical Statistics window at the Connection layer.

The exact information provided in the Statistics window depends both on the Expert layer at which it is displayed and the protocol involved. For example, at the Connections layer, the Statistics window shows the number of requests, number of replies, total bytes, and average frame length on a particular connection. The Statistics window at the Applications layer, however, includes statistics for application requests and average file transfer performance. In general, the Statistics window will quantify and describe network traffic to or from a highlighted station.

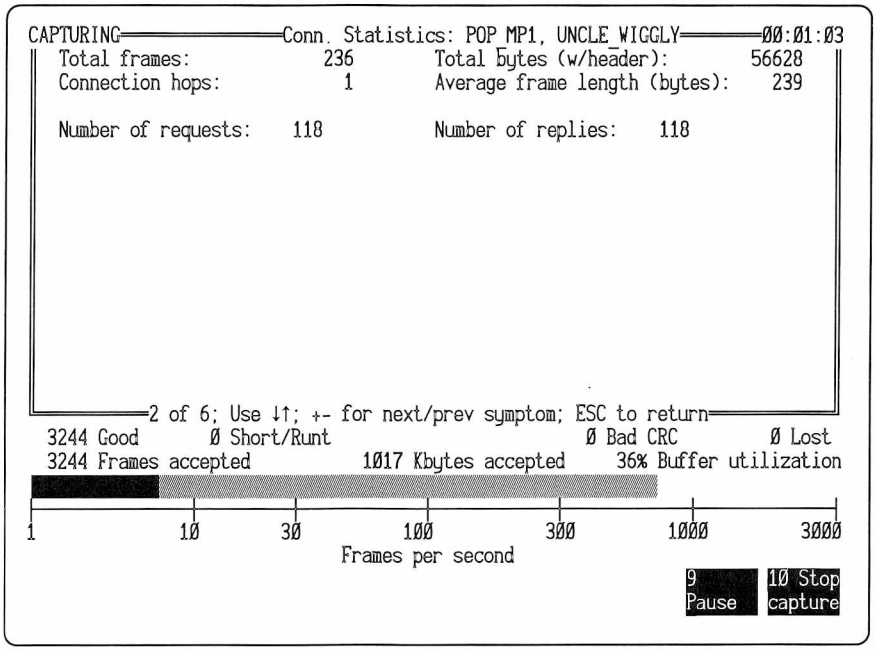


Figure 2–12. Connection Statistics screen

For more information on the various Expert displays available during capture, refer to Chapter 5, "Expert Analyzer Capture and Display."

Protocols Available for Expert Analysis

The Expert Sniffer analyzer can process frames on an Ethernet network segment, a token ring, or a WAN link. Figure 2-14 shows the protocol suites available for the Expert analyzer.

Protocol Family	Constituent Protocols
TCP/IP	IP, TCP, NFS, RPC, TELNET, FTP, ARP, ICMP, RIP, SMB, UDP, IGRP, DNS, X-Window
ISO	Transport layer, CLNP
XNS	XNS, PEP, SPP, NCP, SMB
Novell	PEP, SPX, RIP, SAP, NetBIOS, IPX, NetWare
DECnet	DAP, NSP, DRP, LAT, SMB, SCP, NICE, LAVC
AppleTalk	LAP, DDP, AARP, RTMP, ZIP, NBP, ATP, ADSP, PAP, AFP over ASP
WAN/Synchronous	Frame Relay, X.25, HDLC, IGRP (Cisco), Bridge/Router (various proprietary versions of HDLC)
Banyan VINES	ARP, IPC, ICP, RTP, SPP, StreetTalk

Figure 2–13. Protocols currently available for Expert analysis

The Expert analyzer can perform Classic interpretation on many protocols for which Expert analysis is unavailable. The protocol suites on which your analyzer can perform Expert analysis may vary depending on the topologies installed. The procedure below shows you how to view the protocols for which expert analysis is available.

To view the protocols for which expert analysis is available:

1. Display the Main Menu of the Sniffer analyzer.
2. Use the cursor keys to move to the **Display\Filters\Protocol** menu.
   Result: The menu in Figure 2–14 appears. The analyzer can perform Expert analysis on the protocols marked with an asterisk.

The analyzer can perform Expert analysis on the protocols marked with an asterisk.

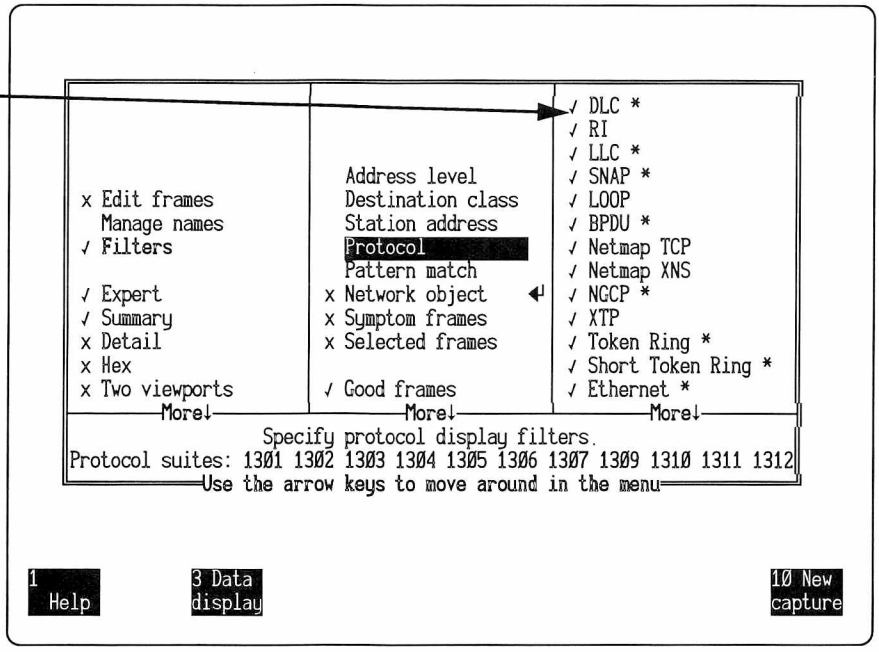


Figure 2–14. The protocols on which the analyzer can perform Expert analysis

Defining System Options and Scheduled Events

3

Defining System Options and Scheduled Events

Overview

To work with system options, you should have successfully started your Sniffer Network Analyzer and attached it to the network. If you have not done so, refer to the *Building the Sniffer Network Analyzer* manual to learn how to install and configure the analyzer.

This chapter explains how to configure the system options in the analyzer's **Options** menu. System options include general network characteristics and general preferences for the analyzer. Some options apply to all networks; others apply only to specific architectures, such as token ring, or to specific platforms, such as the IBM Model 70.

System options for all networks include:

- **Audible clicks**
- **Use defaults**
- **Interpret RI** bit
- **Language**

This chapter also explains the special options available for Ethernet, for token ring, for the IBM PS/2 Model P/70, for the Sniffer Internetwork Analyzer (the Sniffer analyzer for WAN/Synchronous), and for fiber distributed data interface (FDDI) networks.

The **Options** menu is near the bottom of the main menu's first panel. Figure 3–1 shows the menu items in the **Options** menu for Ethernet networks. The **Options** menus for token ring, FDDI, and WAN/Synchronous networks are shown later in this chapter.

NOTE: For the IBM PS/2 Model P/70, the menu includes an additional option for choosing either the external or internal transceiver.

NOTE: The **Automatic Restart** option is not located in the Options menu; it is in the Main Selection Menu. (For more information on the **Automatic Restart** option, see "Automatic Restart Option" on page 11–21.)

This chapter provides an overview of the basic menu items associated with the Options menu. Many of these items, in turn, are associated with additional options. As with all other Sniffer analyzer menu options, you first press the Cursor keys to move the highlight to the desired option. You can then define that option.

- For options marked with the √ and x symbols, you can press Spacebar to enable (√) or disable (x) the option. To reverse all settings, press ALT-Spacebar.
- For options connected with a vertical bar (radio control), you can choose one of those options by moving to it and pressing Spacebar.
- For options where you must define a specific value, you can choose that value from a list or enter the desired value into a dialog box.

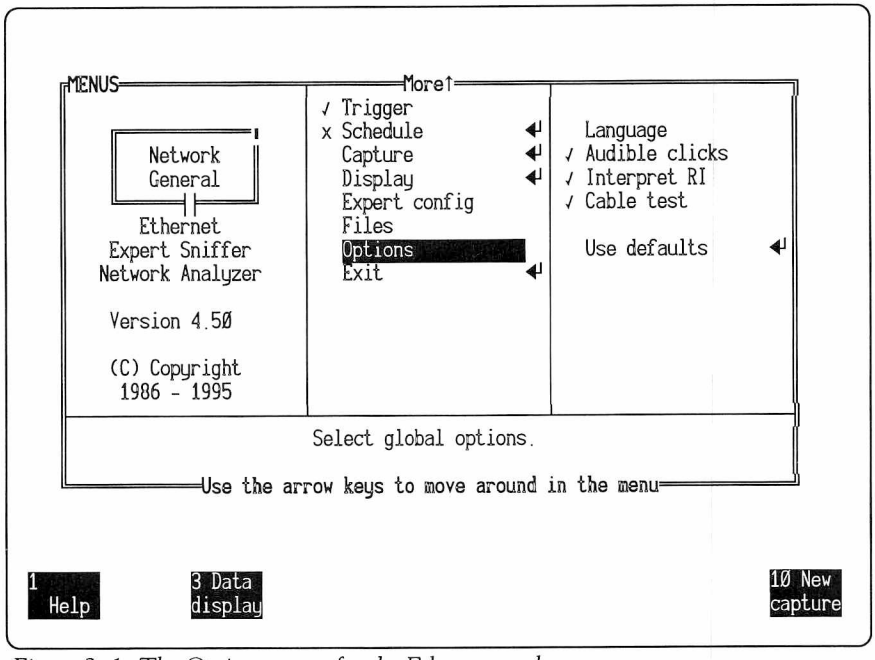


Figure 3–1. The Options menu for the Ethernet analyzer

Setting the Language Option

If you installed the Internationalization update, you can change the language in which the analyzer presents the help and explain files. (To learn how to install the internationalization update, consult the documentation included with it.) The update includes these languages:

- English
- German
- French
- Italian

To set the Language option:

1. Move to **Options\Language**.
2. Highlight the desired language and press Spacebar. The analyzer will display all help and Explain files in this language.

Setting the Audible Clicks Option

The **Audible clicks** option determines whether the Sniffer analyzer "clicks" each time it accepts a frame into the capture buffer. The clicks provide an impression of the general level of traffic, which makes it easy to detect sudden lulls or bursts in traffic without looking at the screen.

With the **Audible clicks** option enabled, the analyzer also clicks each time it transmits a frame during traffic generation.

The default is **√Audible clicks** enabled.

To set or clear the Audible clicks option:

1. Move to **Options\Audible clicks.**
2. Press Spacebar to enable (√) or disable (x) the option.

About the Interpret RI Option

On LAN networks that use six-byte addressing (including token ring and Ethernet), this option determines how the analyzer treats data link connection (DLC) addresses.

Some networks reserve one bit—the RI bit— in the source address to indicate that the frame includes a field called the "source routing information" (RI) field. On networks that recognize the RI bit, an address really consists of only 47 bits. The 48th bit is used in the destination address to indicate "broadcast" or "multicast" and in the source address to indicate "RI present." The broadcast/multicast bit is the bit that is physically transmitted first.[1]

1. This situation occurs because rules for converting bits-on-the-wire to bits-in-memory differ between networks. The broadcast bit is the high-order bit of a token ring address, but in an Ethernet, StarLAN, or PC Network address, it is the low-order bit of the first byte.

RI Fields and "Data Relative" vs. "Frame Relative" Options

IBM introduced source routing on token ring networks, which remains the context in which it is most frequently found. In principle, source routing information can be used not just on token ring but on any LAN that uses six-byte station addresses, including Ethernet, FDDI, StarLAN, and PC Network.

The RI field is a variable-length field inserted after the DLC destination and source fields and before the frame's data field. As a result, the data field is increased by the total length of the RI field. To allow for the varying size of the RI field, you can describe a pattern by either its frame relative or its data relative offset. For more information, refer to "Defining a Pattern Match Filter" on page 6–52.

The RI field contains an identifier for each of the bridges that forwarded the frame. As it retransmits a frame, each bridge appends its own two-byte identifier[1] to the RI field. As a result, the ultimate recipient has a record of all intermediate stations that forwarded the frame.

To request that each intermediary insert its identifier, the originating station turns on the RI bit. In response, each receiving station interprets the first two data bytes as the RI header, perhaps followed by a list of route designator fields.

The originating station sets up the RI header. Five bits in the RI header record the total length of the RI field (including the header). Initially, before the frame is forwarded, the RI field's total length is two bytes. As each bridge forwards the frame it appends its own two-byte identifier, increasing the RI length by two.

Effects of Enabling "Interpret RI"

The default is **Interpret RI** enabled, which means:

- The analyzer treats DLC addresses as 47 bits.
- The analyzer calls the RI interpreter to interpret the RI field of frames that contain this bit in the source address.

A few networks treat all 48 bits as part of the address. On such a network, the 48th bit is part of the address—it does not mean that there is an RI field. When analyzing frames from such a network, disable the **Interpret RI** option. If you do not, the analyzer may try to interpret part of the frame's data field as an RI field.

1. The identifier is composed of a 12-bit ring number and a 4-bit bridge number. These are arbitrary numbers assigned by the network administrators. The RI identifier is unrelated to the bridge's station address.

Effects of Disabling "Interpret RI"

If this option is disabled:

- The Sniffer analyzer treats addresses as 48 bits.
- The analyzer does *not* call the RI interpreter and assumes that there is *never* an RI field.
- The **Destination class** filter continues to recognize the broadcast bit in a destination address. As a result, the filter treats a station whose address includes a one in that position as if it were a broadcast or multicast address.

Setting the Cable Test Option for Ethernet

When you first start capture on an Ethernet analyzer, the analyzer checks to see if it is connected to an Ethernet cable by performing a time-domain reflectometer (TDR) test. The TDR test actually transmits a packet on the cable to verify that it exists. In some isolated cases, this packet may disturb other network activities. You can use the **Cable test** option to disable or enable the initial TDR test.

Resetting all Options

The **Use defaults** option restores the analyzer's default factory settings to all options, including the capture and display filters, triggers, and other options. These settings are stored in the file DEFAULTS.*xx*S, where *xx* is the network abbreviation (such as EN, TR, or FD). For an overview of the factory default settings of all options, refer to the *Quick Reference Card* included with your documentation.

NOTE: *Do not* alter the settings in DEFAULTS.xxS—it allows you to always start from a known state. If you want to apply the settings you define at system startup, save them to the STARTUP.*xx*S file in the C:\xxSNIFF directory.

To restore the system defaults:

1. Move to **Options\Use defaults** and press ENTER.

WARNING. If you use this option, you will clear any settings you may have defined. If you want to use those settings later, save the current settings as a Setup file. For details, refer to "Using Setup Files to Define System Options" on page 8–21.

Setting the Transceiver Option for the IBM PS/2 Model P/70

On an Ethernet Sniffer analyzer, IBM's Microchannel technology makes it possible to use software to change between BNC and AUI ports, without having to remove the adapter card and change a jumper block.

If you run the analyzer with an Ethernet-II adapter card on the Model 70, you can choose whether to use the external transceiver attached to the DB-15 connector, or the internal transceiver that uses the thin Ethernet BNC connector. Therefore, if you use the AUI ports, choose the External transceiver option; if you use the BNC port, choose the Internal transceiver option. If you want to switch between the two options, connect to the appropriate port.

IMPORTANT: *Do not* physically connect to both ports simultaneously and then try to switch between ports by using this option. If you do so, you risk crosstalk between the segments attached to each port, or even network failure.

The default is **External transceiver** selected.

To choose between ports on the Model 70:

1. Move to **Options** and then to the desired transceiver and press Spacebar.

   ▶External transceiver
   Internal transceiver

Setting the Token Ring Options

On a token ring Sniffer analyzer, the **Language**, **Audible clicks**, **Interpret RI**, and **Use defaults** options operate as they do on an Ethernet network, as described in the previous section. Token ring networks also include these additional system options:

- **Network speed** (4 Mb/S or 16 Mb/S)
- **Remove from ring** if there is no signal (Token Ring-III only)
- **Force open** option (Token Ring-II only)

Figure 3–2 shows the system options associated with a token ring analyzer.

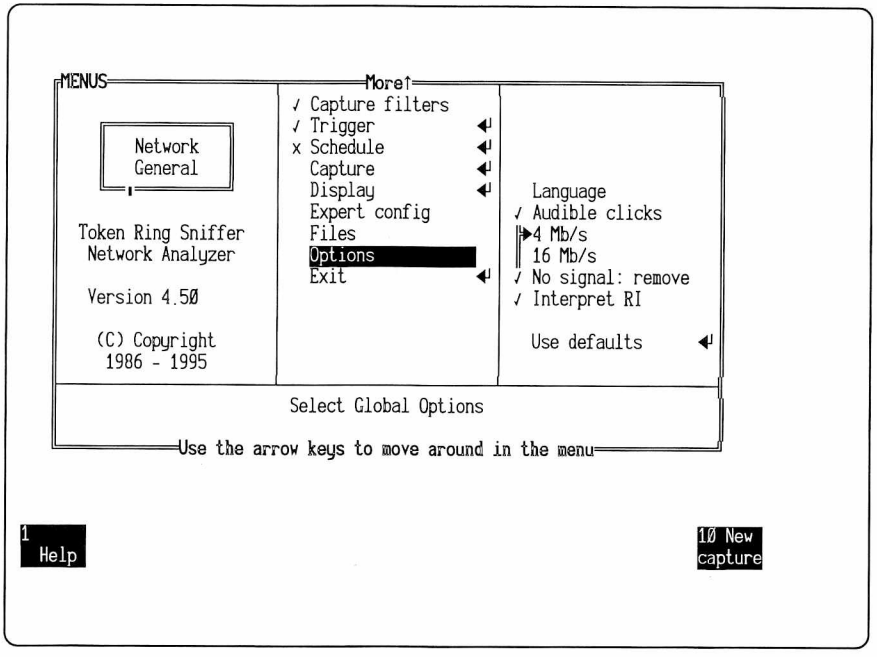


Figure 3–2. The Options menu for the token ring analyzer

Setting the Token Ring Speed

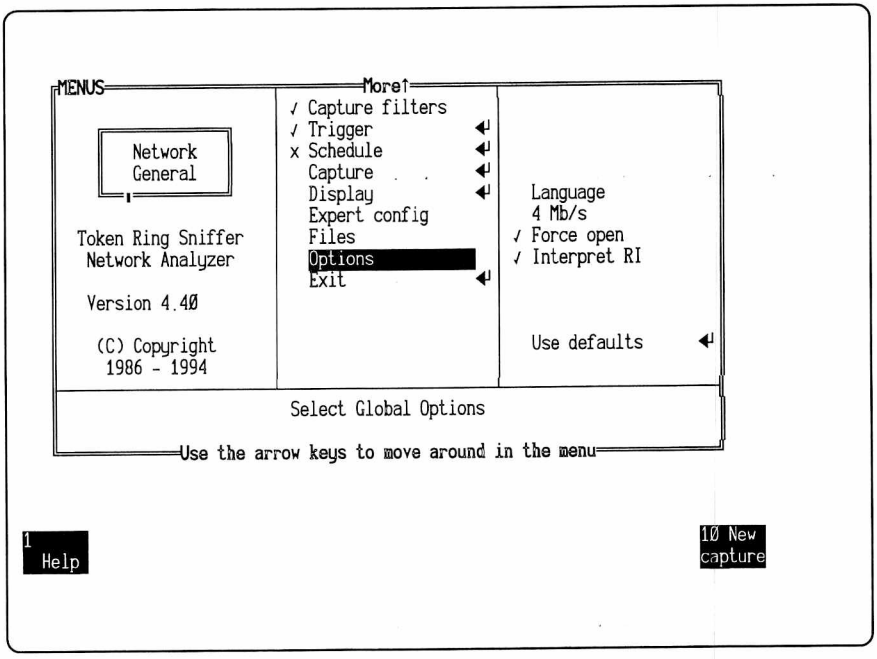


Figure 3–3. Setting the token ring speed

How you set the speed of your token ring analyzer depends on what version of the analyzer you have. There are three versions described below:

If you have a Token Ring 16/4 Network Analyzer

The Token Ring 16/4 adapter card is capable of capturing from networks running at speeds of either 4 or 16 Mbps. If the wrong speed is selected, the ring will be disrupted, although you can minimize the disruption by enabling the **No signal: remove** option, as described in the next section.

If you move the Sniffer analyzer to another network, you can use the speed options to select the appropriate speed.

To set the network speed used by the analyzer's adapter card:

1. Move to **Options** and then to the desired speed and press Spacebar.

   ▶4 Mb/s
   16 Mb/s

NOTE: You can choose from the menu the speed at which you want to capture. On the Model 70, you can also select the speed for traffic generation from the menu. For

other analyzer platforms, however, you must set a switch on the token ring adapter card for the correct transmission speed.

If you have a Token Ring-II Analyzer:

Token Ring -II uses Madge Network's "Smart 16/4 AT Ringnode" board as the network adapter. In most of the previously released token ring analyzers, token ring speed for frame capture was set by a menu selection, whereas token ring speed for traffic generation had to be set by changing a switch setting on the network adapter card. In the Token Ring-II analyzer, token ring speed (for both frame capture and traffic generation) is determined by a selection in the **Options** menu (as in the procedure above). However, the **No signal: remove** option (which in earlier models prevented the analyzer from entering a ring at the wrong speed or during a ring beacon condition) is not present in Token Ring-II.

The Ringnode board is shipped by Network General with the token ring speed DIP switch set for 4 Mbps. This setting enables the software control mentioned above to select either 4Mbps or 16 Mbps. If this switch were set to 16 Mbps, then you can only use the analyzer at 16 Mbps.

If you have a Token Ring-III Analyzer:

Token ring speed for frame capture is determined by a selection in the **Options** menu of the Token Ring-III analyzer (as described in the procedure above).

The token ring speed for traffic generation in the analyzer, and for the station test and token timer features in the monitor, is determined by a line in the CONFIG.SYS file, according to the setting of the ring speed parameter (RS). The installation procedure sets the ring speed for traffic generation to 16Mbps, by creating this line in CONFIG.SYS:

```
device=c:\tools\pointtr.sys SB RS=16 IRQ=3 ...
```

To set the traffic generation ring speed to 4 Mbps, change RS=16 to RS=4:

```
device=c:\tools\pointtr.sys SB RS=4 IRQ=3 ...
```

If you edit this line, reboot your notebook computer when you are finished editing.

Token Ring Remove Option for Token Ring-1 Analyzer

With a token ring network running the Token Ring-I (IBM 16/4) adapter, you can determine how the analyzer responds if it receives no signal when it inserts itself into the ring. There are two choices: it can remove itself from the ring immediately or remain in the ring.

IMPORTANT: Removing the analyzer minimizes disruption if you inadvertently connect an analyzer configured for one transmission speed to a ring that operates at a different speed.

However, operating without automatic removal has two advantages:

- When the ring is broken, you can connect to a portion of the ring and await signals as you make other changes to the ring.
- On a functioning ring, you can disconnect temporarily and reconnect without having to reset the analyzer's adapter card.

If you are certain that the analyzer's speed matches the network speed, you can remove this protection.

The default is **No signal: remove** enabled.

Force Open Option for the Token Ring-II Analyzer

The **Options** menu on the Token Ring-II (Madge) analyzer includes a **Force open** option.

- When this option is enabled, the analyzer can enter a beaconing ring by sending a **Force open** command to the network adapter. When the analyzer enters the ring, it may become the active monitor.
- When this option is disabled, the analyzer cannot enter a beaconing ring.

The default is **Force open** disabled.

Setting the Sniffer Internetwork Analyzer Options

On a Sniffer Internetwork (WAN/Synchronous) Analyzer, the **Audible clicks**, **Interpret RI**, and **Use defaults** options operate as they do on an Ethernet network, described in the previous sections. The Sniffer Internetwork Analyzer includes several additional system options:

- Frame type options
- Encoding method options
- Physical line interface options

Figure 3–4 shows the system options associated with the Sniffer Internetwork Analyzer. Each is described in the sections below.

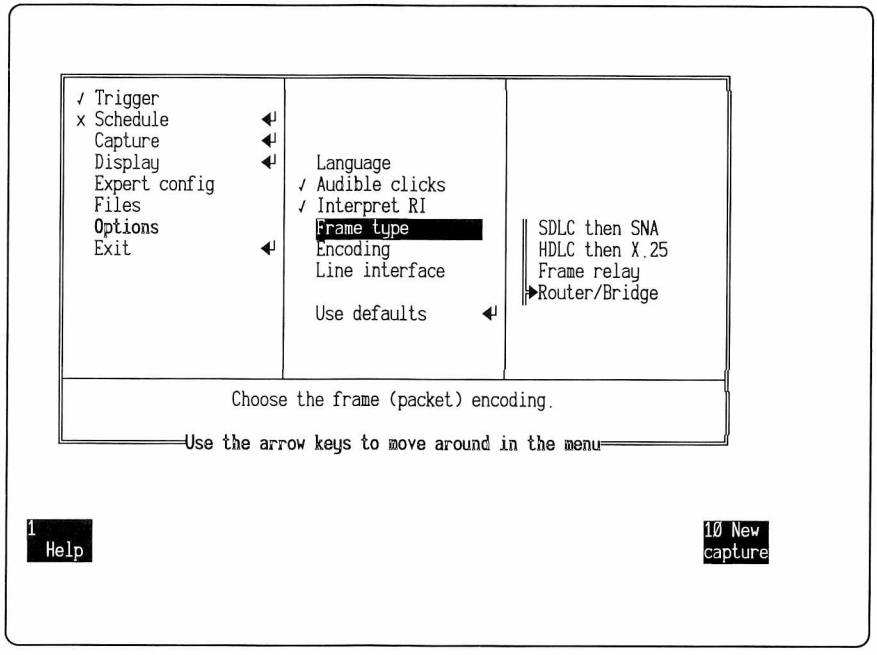


Figure 3–4. The Options menu: WAN/Synchronous analyzer

Frame Type Options

If you have a WAN/Synchronous network, you will need to define the lower-level protocols used by the synchronous link. This includes defining the frame type and the encoding method used to transmit the frame across the WAN.

The **Frame type** options let you define the access protocols, including Frame relay, Router/Bridge, SDLC/SNA (IBM's Synchronous Data Link Control protocol), and HDLC/X.25 (High-level Data Link Control). None of these protocols affect which of the higher-level protocols are embedded within their frames.

Of these protocols, the most widely used are SNA (System Network Architecture) over SDLC at IBM installations, and X.25 over HDLC, which is widespread in Europe and is used increasingly in the United States. The Frame relay frame type is widely used for LAN interconnectivity, as are proprietary versions of HDLC (decoded by the **Router/Bridge** option). For examples of how these options determine what is displayed during capture, see "Frame Counts Display During Capture: WAN/Synchronous" on page 6–23.

The default frame type is **Router/Bridge**. The **Router/Bridge** option lets the analyzer decode proprietary versions of HDLC during capture. Many leased-line internetworks use proprietary versions of HDLC. The Sniffer Internetwork Analyzer can recognize

and interpret data within many versions of HDLC. These include the Point-to-Point (PPP) standard router/bridge frame format and also a variety of others, including proprietary versions of HDLC from the following router/bridges:

- Wellfleet (Versions 3.1, 3.3, and 3.7)
- Cisco
- Vitalink
- Proteon
- IBM source routing bridges (Versions 2.2 and 2.3, token ring only)
- Microcom

NOTE: For Microcom bridges, **Encoding** must be set to **Modulo-128** rather than **Modulo-8**.

- Ungermann-Bass
- ACC
- Banyan Vines
- Crosscom
- Retix
- DEC
- Netronix
- ATT

NOTE: If your analyzer has a color display, the Sniffer Internetwork Analyzer displays proprietary router/bridge information in black.

IMPORTANT: If the Sniffer Internetwork Analyzer does not automatically recognize the bridge, router, or protocol in use, you can use the analyzer's **Protocol forcing** feature to force the interpretation of non-standard protocols. For more information on this feature, see Chapter 9, "Using Protocol Forcing."

If you notice during display that the wrong frame type is displayed, return to the **Options\Frame type** menu and choose the correct frame type. To apply the new interpretation to a set of captured frames, you must reinterpret the frames. You can reinterpret the frames by pressing F6 **[Display Options]**, highlighting the **Reinterpret** option, and pressing ENTER. The frames will be reinterpreted in accordance with the new settings.

Encoding Options

Associated with the **Frame type** options are the schemes for encoding frames and the data bits within frames of transmitted data. This includes whether or not to invert the

data bits, the method for generating the sequence number of the frames, and the decoding method itself.

Inverting Data Bits

Some WAN/Synchronous networks invert data bits as they come off the wire (changes binary 0 to 1, and vice versa). To make sure the analyzer reads the data correctly, enable the **Invert** option, which corrects for inversion to read the data correctly.

About WAN/Synchronous Frame Numbering

There are two methods for generating frame sequence numbers. Which of these methods is used is not readily distinguishable by inspection. The method that uses three bits (Modulo 8) is widely used in the United States and in Europe. The method that uses seven bits (Modulo 128) is often used in Japan and in international satellite links.

The default is √ **Modulo 8** enabled.

About WAN/Synchronous Data Signaling

The two most common encoding methods for SDLC and HDLC are NRZ (Non-return to zero) and NRZI (Non-return to zero inverted). To decode transmitted data correctly, you should define the encoding method.

The default is √ **NRZ** enabled.

16-Bit or 32-Bit CRC

The Sniffer Internetwork Analyzer can now decode16-bit CRC and 32-bit CRC for communications between two routers. The default is 16-bit CRC.

Line Interface Options

The Sniffer Internetwork (WAN/Synchronous) analyzer provides several options for the physical line interface, including:

- RS-232 interface via a DB-25 cable
- RS-422 interface via a DB-15 cable
- RS-423 interface via a DB-15 cable
- V.10 interface via a DB-15 cable
- V.11 interface via a DB-15 cable
- V.35 interface via a DB-15 cable
- T1 interface via the Network General T1-POD
- E1 interface via the Network General E1-POD

NOTE: The Network General T1-POD and E1-POD are supplied separately. They are not included with the Sniffer Internetwork Analyzer. For more information on the T1-POD and E1-POD, see the documentation accompanying those products.

The default is the V.35 interface via a DB-15 cable. For complete information on the physical line interfaces supported by the Sniffer Internetwork Analyzer, see *Building the Sniffer Network Analyzer*.

Setting the FDDI Options

On an FDDI Sniffer analyzer, the **Audible clicks**, **Interpret RI**, and **Use defaults** options operate as they do on an Ethernet network, as described in the previous sections. FDDI networks include two additional system options: the station mode and the option to invert addressing.

Figure 3–5 shows the system options associated with an FDDI analyzer.

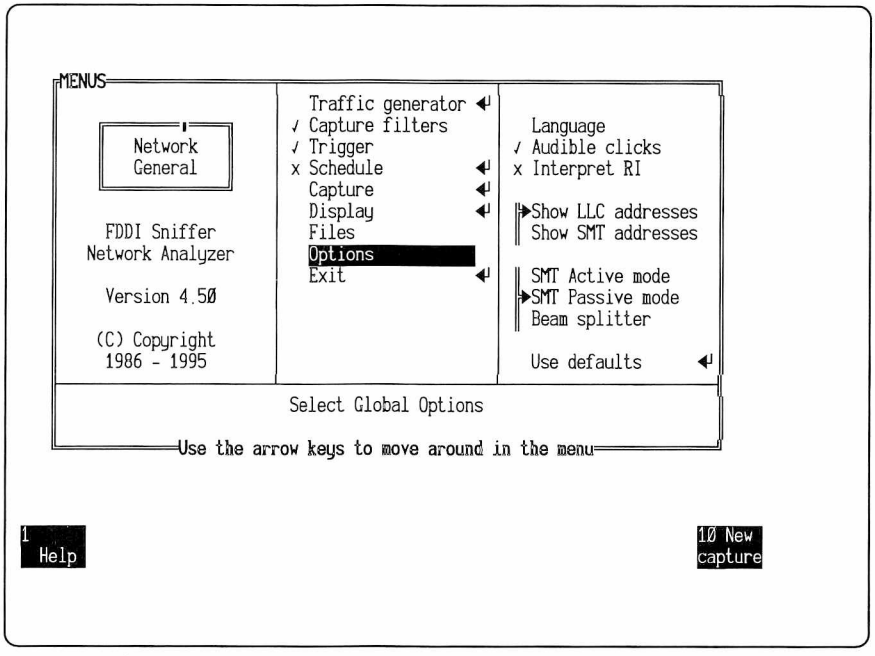


Figure 3–5. FDDI options

Setting the Station Mode

You can set the FDDI analyzer as an SMT Active station, an SMT Passive station, or a beam splitter on the FDDI ring.

Setting the analyzer as an SMT Active station means that it participates in the FDDI network activity. It periodically sends out neighbor information frame (NIF) announcements and responds to its upstream neighbor's NIF requests. A monitoring station can use these announcements to construct an SMT ring map.

Setting the analyzer as an SMT Passive station means it has a more limited involvement with the ring. It participates at the MAC and CMT levels, and forwards frames, but it does not send NIF announcements and responses, and thus it will not appear in an SMT ring map.

Setting the analyzer as a beam splitter means that it is completely passive and does not participate in any ring activity. You must connect your analyzer to the network via a beam splitter in order to use this setting.

When a beam splitter is used, the maximum length between FDDI stations is considerably less than the standard 2km for multimode fiber. This is due to the signal loss caused by splitting the beam. The vendor of the beam splitter device should specify the signal loss.

Inverting Addresses

From the perspective of the FDDI analyzer, each station uses two logical addresses to communicate. One form of the address is the canonical form of the assigned DLC address. The other is the most significant bit (MSB) form. When a station transmits LLC frames, the analyzer sees the canonical form of its assigned DLC address. However, when the same station transmits SMT or MAC frames, the analyzer sees the MSB form of its DLC address.

The **Show LLC addresses** or **Show SMT addresses** option allows you to display the FDDI station addresses using one of the two logical addresses. This option affects all displays except the HEX view where data is presented as provided by the FDDI interface card (that is, with MAC and SMT frame addresses in MSB form and LLC frame addresses in canonical form– see the paragraph below).

The analyzer's FDDI interface card presents LLC frame addresses to the Sniffer analyzer in canonical form. Consequently, the HEX view shows all LLC frame DLC addressesin canonical form regardless of the **Options** setting. MAC and SMT frame DLC addresses are always displayed in the HEX view in MSB form.

The default is **Show LLC addresses** enabled (display station addresses using LLC addresses). This option only affects the way DLC addresses are displayed in the Summary and Detail views. The HEX view is unaffected by the setting of this option.

Figure 3–6 illustrates how this feature works. In this example, the assigned IEEE burned-in DLC address is 01-01-01-01-01-01 (the canonical form).

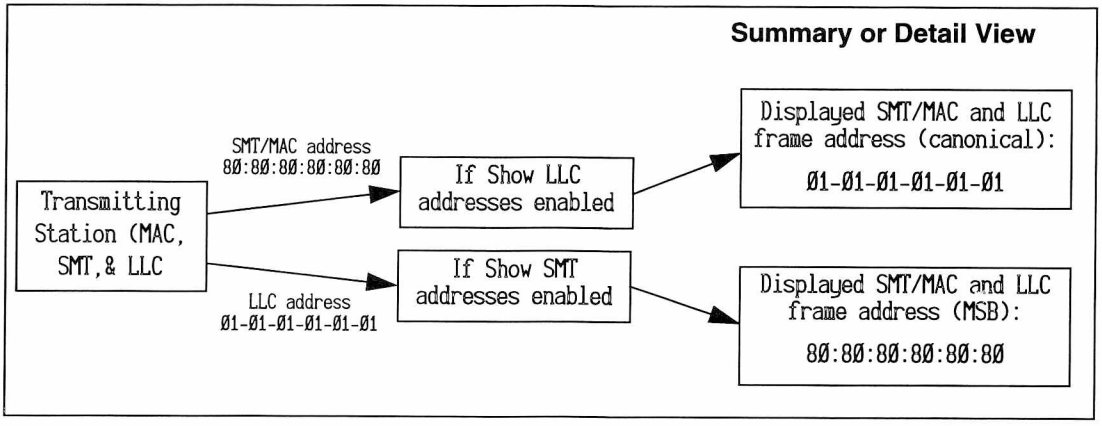


Figure 3–6. Show LLC or SMT addresses option

If you set a capture or display filter or a trigger, make sure that the DLC address you enter matches the option setting you selected. If not, your filter or trigger will not work. For example, if the canonical form of a station address is 00-00-65-0A-00-01 (SMT address is 00:00:A6:50:00:80), and the option is set to **Show LLC addresses**, make sure you use the canonical form of the DLC address for any station capture or display filter or trigger. If you use the SMT address, the analyzer will assume that you are entering an LLC address, and the filter or trigger will not work.

Scheduled Events

Overview

You can schedule your analyzer to perform scheduled events each week, including:

- Saving the Expert database in CSV (comma separated values) file format
- Saving the contents of the capture buffer into a trace file
- Clearing the Expert database and resetting the global statistics
- Clearing the analyzer's name table
- Loading the startup name table
- Loading a new setup file

The Scheduled Events Table

To schedule an event, select **Schedule** from the analyzer's main menu. A screen similar to the one in Figure 3–7 will appear:

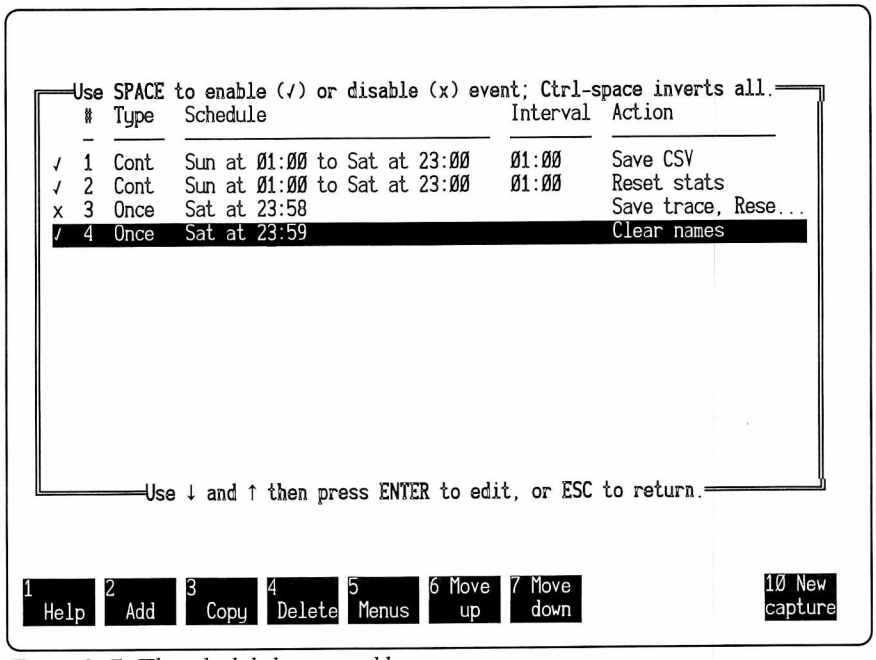

Use SPACE to enable (/) or disable (x) event; Ctrl-space inverts all.
Type Schedule Interval Action
/ 1 Cont Sun at 01:00 to Sat at 23:00 01:00 Save CSV
/ 2 Cont Sun at 01:00 to Sat at 23:00 01:00 Reset stats
x 3 Once Sat at 23:58 Save trace, Rese...
/ 4 Once Sat at 23:59 Clear names
Use ↓ and ↑ then press ENTER to edit, or ESC to return.
1 Help
2 Add
3 Copy
4 Delete
5 Menus
6 Move up
7 Move down
10 New capture

Figure 3–7. The scheduled events table

If no events are scheduled, the screen will say <Use Add key to add a new event>, and you can press F2 to schedule the first event. If there are multiple events scheduled, the screen will look like the one in Figure 3-6.

If two events are scheduled for the same time, they will occur in the order in which they appear in the list. Therefore, list events so you get the actions you want. For example, **Reset statistics** followed by **Save CSV** will not save the Expert database, but the same events in the opposite order will save the Expert database and then start on a new one.

You can move the highlight up and down with the arrow keys. When an event is highlighted, you can toggle between the enabled and disabled states by pressing the Spacebar. You can use the function keys to move, copy, or delete the highlighted event, or to add a new event. To modify an existing event, highlight it and press ENTER.

When you press F2 to add an event, or when you select an existing event to modify, the CONFIGURE EVENT screen appears.

Again, you can toggle the event between the enabled and disabled states by pressing the Spacebar when **Enabled** is highlighted. This has the same effect here as on the previous screen.

Choosing When an Event Occurs

To specify when an event should occur, move the highlight to the **Weekly Schedule** selection. The Configure Event screen looks like this:

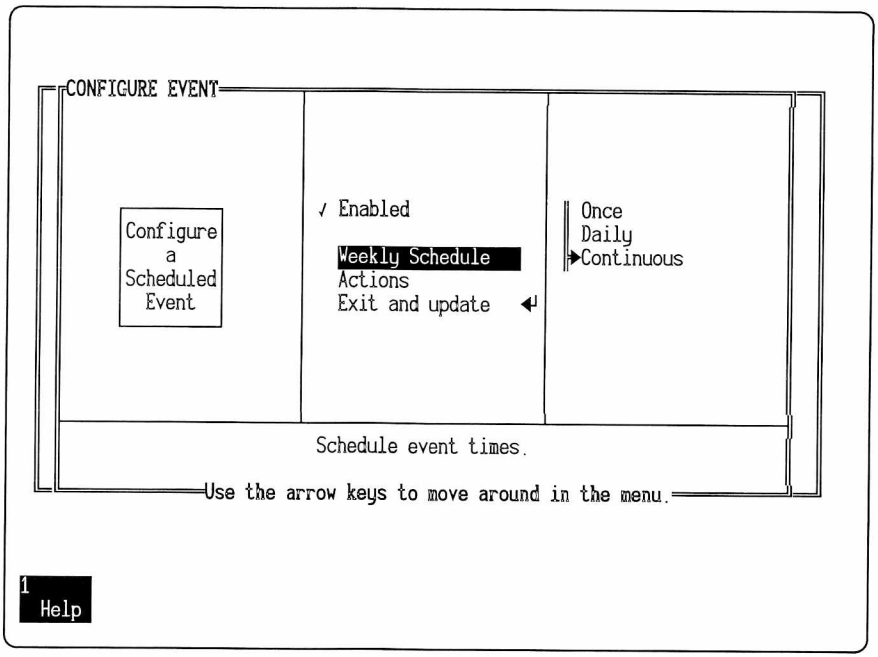


Figure 3–8. Three schedule modes

The **Weekly Schedule** selection lets you specify when the scheduled events should occur. Whatever schedule you set up will repeat every week. However, the scheduled events will occur only when the analyzer is actually capturing frames (from a network or from a trace file) in Expert mode or in Classic mode.

Within the **Weekly Schedule** function, you can choose:

Once	Schedules an event to occur at a specific time each week.
Daily	Schedules an event to occur repetitively, on days of the week you select. You enter the starting and ending time of day, and the interval between events. **If the ending time is earlier than the starting time, the analyzer will end the event on the next day.**

Continuous	Schedules an event to occur repetitively. You enter a beginning day of the week and time of day, an ending day and time, and the interval between events.

You select a scheduling basis by highlighting it and pressing the Spacebar. When you highlight a selection, you will see a submenu that lets you set the various time parameters involved.

Scheduling Events in Greenwich Mean Time

To schedule events in Greenwich Mean Time (GMT), move to **Schedule\GMT Time** and press the Spacebar to enable the GMT option. (To use the GMT option, make sure your system time and the DOS environment variable TZ are set correctly.)

Choosing What Actions are Performed

After you have chosen the time basis for your scheduled event, you can then specify what actions you want to occur at those times. When you highlight the **Actions** selection, the screen looks like this:

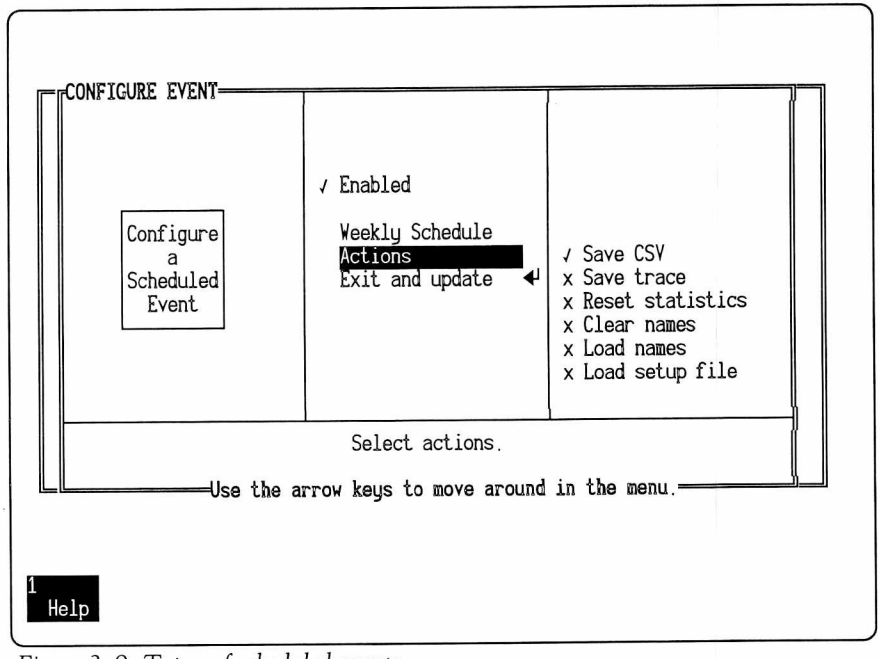


Figure 3–9. Types of scheduled events

You can select more than one event to occur at the specified times. Simply enable or disable the events using the Spacebar.

If you enable two or more items in the **Actions** menu, then at each event time those actions will be performed in the order listed in the menu.

Save CSV and **Save trace** actually occur at the end of each configured interval; all the other event types occur at the beginning of each interval.

The following sections describe the available actions.

Save CSV

The **Save CSV** action saves information from the Expert database to a file in CSV file format. The file will be created in the *xx*REPORT directory, where *xx* represents the network adapter type — for example, ENREPORT for Ethernet. The analyzer will automatically assign a filename of the form

XP*mddttt*.CSV

where

m is the month (hexadecimal notation — Jan = 1, ... , Dec = C)

dd is the day of the month (hexadecimal)

ttt is the time of day in minutes (hexadecimal)

The specific categories of Expert information saved — thresholds, global statistics, Expert overview, network objects, and or diagnoses — are determined by the options enabled in the **Files\Save\Expert data** submenu at the time the **Save CSV** event occurs.

The **Save CSV** function works only in Expert capture mode.

Save trace

The **Save trace** action saves the frames in the capture buffer to a trace file. The file will be created in the \CAPTURE directory. The analyzer will automatically assign a filename of the form

TR*mddttt.xx*C

where

m is the month (hexadecimal notation — Jan = 1, ... , Dec = C)

dd is the day of the month (hexadecimal)

ttt is the time of day in minutes (hexadecimal)

xx is the network adapter type — for example, EN for Ethernet

The specific frames saved are determined by the options enabled in the **Files\Save\Data** submenu at the time the **Save trace** event occurs.

When you enable **Save trace** it automatically also enables **Reset statistics**.

Reset statistics

The **Reset statistics** action clears the Expert database and resets the global statistics.

Clear names

The **Clear names** action deletes all the names and addresses from the working name table in memory.

Load names

The **Load names** action reloads the name table that was loaded during analyzer startup.

Load setup file

The **Load setup file** action loads a new setup file. To specify the name of the setup file, move to "**File=**" and press ENTER. Then select the file from the list that appears. The extension will have been appended automatically when the setup file was saved, and will be of the form *xx*S, where *xx* represents the network adapter type — for example, EN for Ethernet.

When you enable **Load setup file** it automatically also enables **Reset statistics**.

A setup file contains the enabled/disabled status of all menu items. When you schedule a **Load setup file** event, pay particular attention to how the enabled/disabled flag is set on the **Schedule** item in the main menu. If you load a setup file with the **Schedule** item disabled, then the analyzer will not execute scheduled events.

Updating the Scheduled Events Table

After you have chosen the time(s) and action(s) for an event, you can update the scheduled events table by moving the highlight to **Exit and Update** and pressing ENTER. You can then schedule more events, or press ESC or F5 to return to the main menu.

The SCHEDULE.CFG File

The information in the scheduled events table is saved to the SCHEDULE.CFG file in the \CONFIG directory when you exit the analyzer. When you restart the analyzer, it reads SCHEDULE.CFG and loads the events in the scheduled events table.

Defining Expert Analyzer Options

4

Defining Expert Analyzer Options

Overview

This chapter explains the network layering scheme the Expert analyzer uses to categorize network problems and describes various precapture Expert options, including:

- How to specify TCP/IP subnet masks using the Expert analyzer's configuration function. You must be careful to configure the Expert analyzer with the subnet mask appropriate to the network it is analyzing. Configuring the Expert analyzer with an incorrect subnet mask can result in spurious symptoms and diagnoses in a TCP/IP environment.
- How to specify common Trustee names that should be excluded from the Expert analyzer's name search in a Novell environment.
- How to set Expert thresholds: You can adjust the Expert thresholds to control when the analyzer reveals symptoms and diagnoses.
- How to use the **Recycle Objects** option. This option helps you to use memory and processor time optimally, in accordance with your network analysis needs.

The chapter also describes how the analyzer learns the symbolic names of network entities by extracting relevant information from captured packets. When the analyzer learns a symbolic name, it will substitute that name for the address in the Expert displays. Several "tricks" to speed this process are discussed at the end of this chapter.

Expert Layers and the OSI Model

The Expert analyzer categorizes network problems according to the Expert layer at which they occur. During capture, the Expert analyzer uses its real-time protocol interpreters to map the information embedded in each frame onto its own model of network layers.

IMPORTANT: The network layering structure on the Expert analyzer is similar to the OSI model. However, the two schemes do not always exhibit a one-to-one mapping. Figure 4–1 explains what each Expert layer means and how it corresponds to the layers in the OSI model.

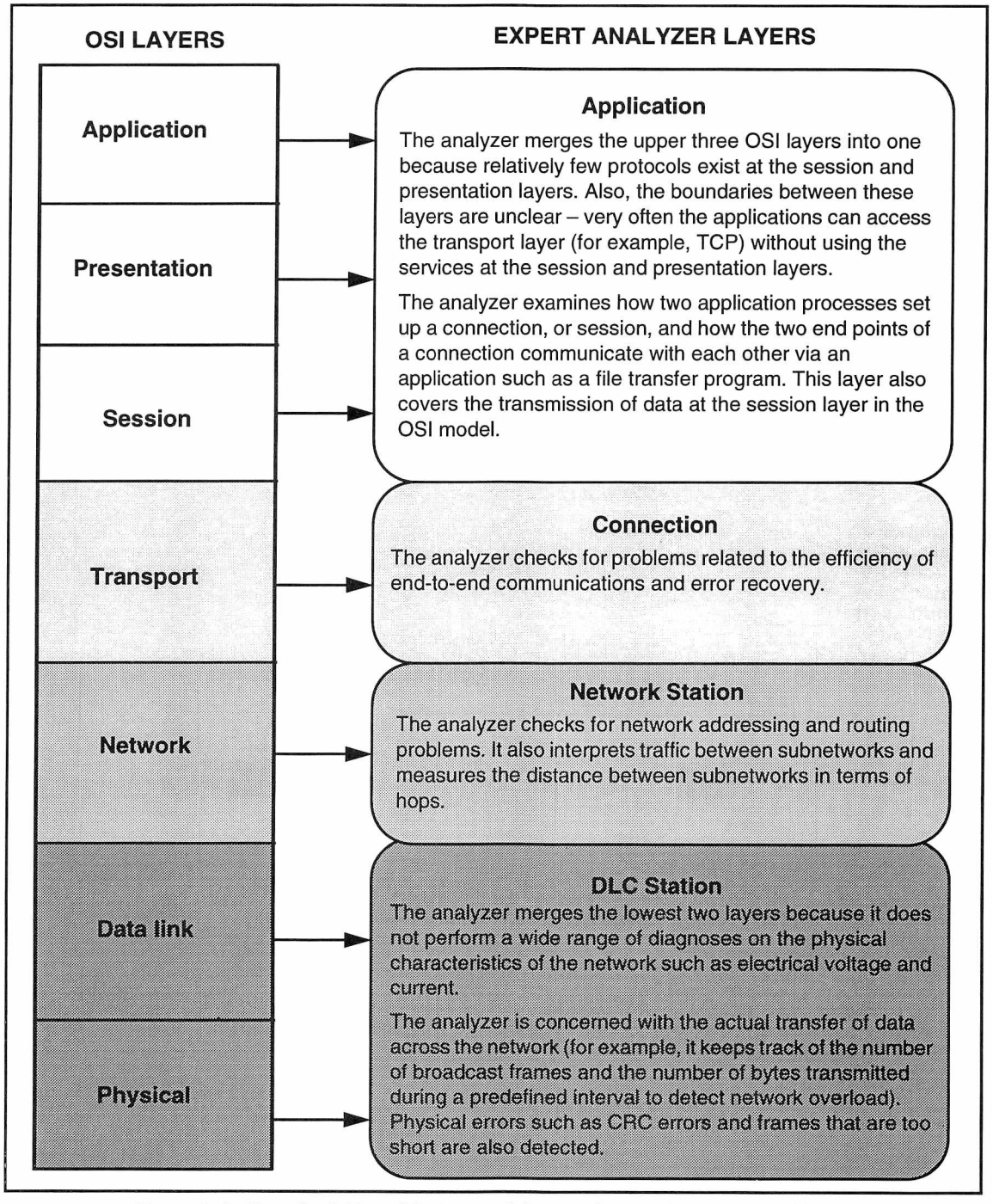

OSI LAYERS
EXPERT ANALYZER LAYERS
Application
Presentation
Session
Transport
Network
Data link
Physical
Application
The analyzer merges the upper three OSI layers into one because relatively few protocols exist at the session and presentation layers. Also, the boundaries between these layers are unclear – very often the applications can access the transport layer (for example, TCP) without using the services at the session and presentation layers.
The analyzer examines how two application processes set up a connection, or session, and how the two end points of a connection communicate with each other via an application such as a file transfer program. This layer also covers the transmission of data at the session layer in the OSI model.
Connection
The analyzer checks for problems related to the efficiency of end-to-end communications and error recovery.
Network Station
The analyzer checks for network addressing and routing problems. It also interprets traffic between subnetworks and measures the distance between subnetworks in terms of hops.
DLC Station
The analyzer merges the lowest two layers because it does not perform a wide range of diagnoses on the physical characteristics of the network such as electrical voltage and current.
The analyzer is concerned with the actual transfer of data across the network (for example, it keeps track of the number of broadcast frames and the number of bytes transmitted during a predefined interval to detect network overload). Physical errors such as CRC errors and frames that are too short are also detected.

Figure 4–1. How the OSI model of network layers relates to the Expert model

The Expert analyzer's model of network layers is shown in the Expert Overview, illustrated in Figure 4–2. From this window, you can view subdisplays associated with network objects, symptoms, and diagnoses detected at the various Expert layers. For more information on the displays available in the Expert window, see Chapter 5, "Expert Analyzer Capture and Display."

NOTE: In addition to the four Expert layers, the Expert Overview also tallies Global Symptoms and Subnet Pairs. Global Symptoms are those symptoms which do not reside at any particular layer, such as Broadcast Storms. Subnet Pairs provides information on all communicating subnets the Expert analyzer detects. These displays are described further in Chapter 5, "Expert Analyzer Capture and Display."

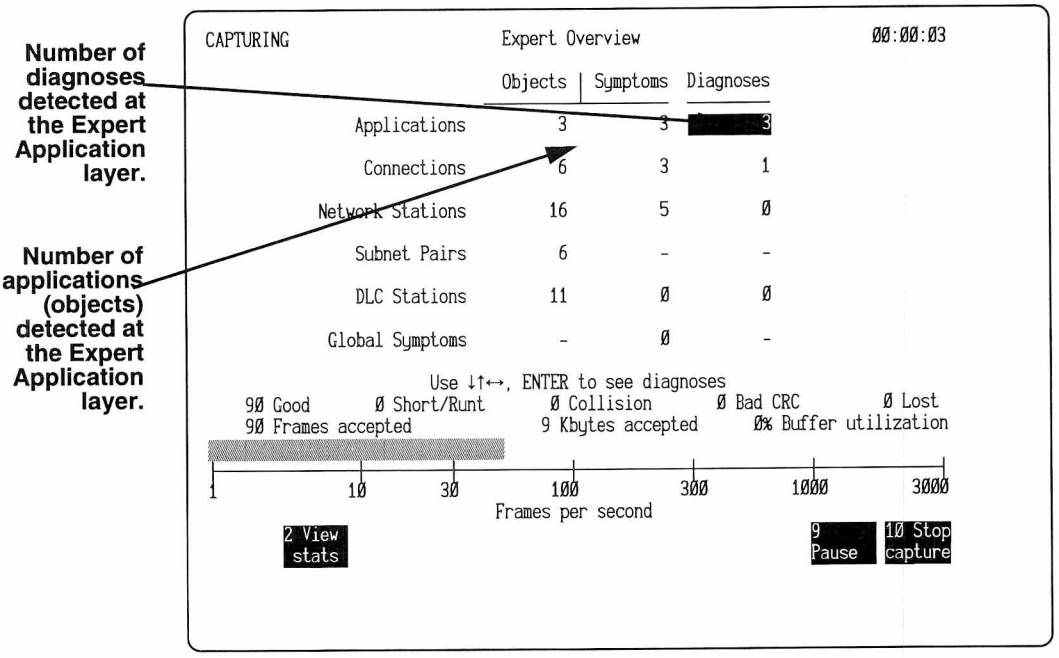

Number of diagnoses detected at the Expert Application layer.
Number of applications (objects) detected at the Expert Application layer.
CAPTURING
Expert Overview
00:00:03
Objects | Symptoms | Diagnoses
Applications 3 3 3
Connections 6 3 1
Network Stations 16 5 0
Subnet Pairs 6 - -
DLC Stations 11 0 0
Global Symptoms - 0 -
Use ↓↑↔, ENTER to see diagnoses
90 Good 0 Short/Runt 0 Collision 0 Bad CRC 0 Lost
90 Frames accepted 9 Kbytes accepted 0% Buffer utilization
1 10 30 100 300 1000 3000
Frames per second
2 View stats
9 Pause
10 Stop capture

Figure 4–2. The Diagnosis Overview window. The four Expert layers are displayed at left, along with Subnet Pairs and Global Symptoms.

The Expert layering structure is also used to group thresholds for symptoms and diagnoses in the **Expert config** menu. For more information on Expert thresholds, see "Setting Thresholds for Symptoms and Diagnoses" on page 4–13.

Configuring the Expert Analyzer

For effective network analysis, configure these two options before capture begins. (Whether or not you need to configure these options depends upon the network's protocol environment.)

- Subnet Masks — Must be configured for a TCP/IP environment.
- Trustee Names — Can be configured for a Novell environment.

To configure these items, use the Expert analyzer's **Expert config** menu. The changes made with the configuration function are saved to the appropriate STARTUP.*xx*V file (where *xx*=EN for Ethernet, TR for token ring, or SY for WAN/Synchronous).

Figure 4–3 shows the Expert analyzer's **Expert config** menu.

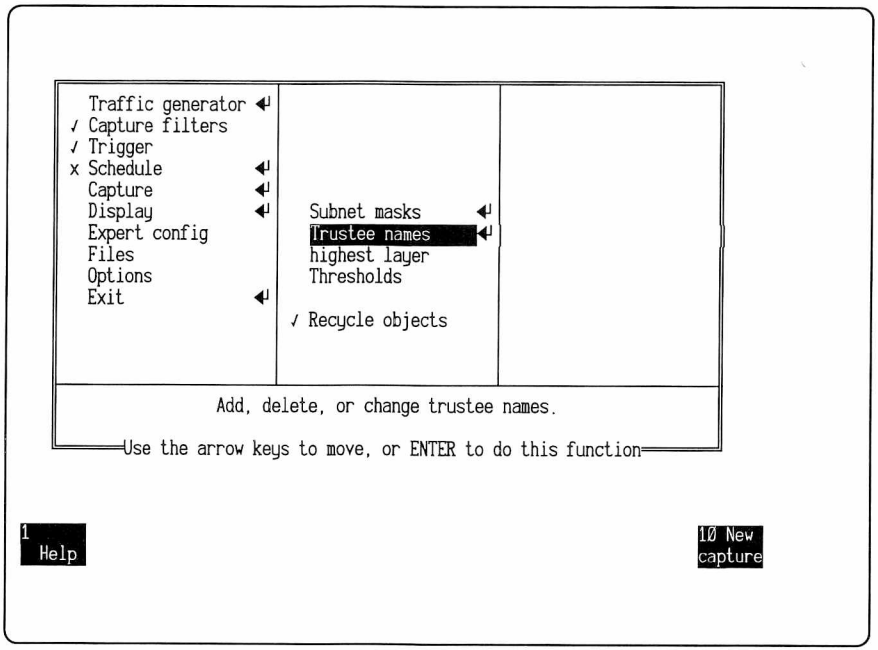


Figure 4–3. Expert config menu of the Expert Sniffer analyzer

Setting Subnet Masks

A traditional standard of TCP/IP subnet masks exists, which reserves specific bits within an IP network address for the subnet mask, depending on the class of address. The Expert analyzer comes with default subnet mask settings for each class of IP address:

IP Address	Expert Default Subnet Mask
Class A	[255.255.0.0]
Class B	[255.255.255.0]
Class C	[255.255.255.0]

IMPORTANT: Networks may use non-traditional subnet masks. If the Expert analyzer is attached to a network segment which uses non-traditional subnet masks, it is possible that the analyzer will register spurious network objects and diagnoses. This happens because the analyzer expects address information at a location within the address field other than where it actually is.

Example: Using an Incorrect Subnet Mask

Figure 4–4 shows two different legal Class A IP broadcast addresses.

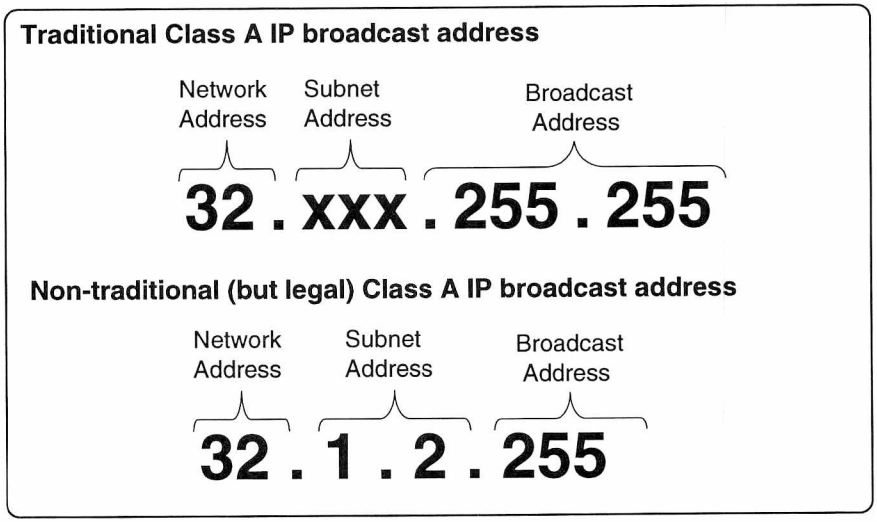

Traditional Class A IP broadcast address
Network Address
Subnet Address
Broadcast Address
32 . xxx . 255 . 255
Non-traditional (but legal) Class A IP broadcast address
Network Address
Subnet Address
Broadcast Address
32 . 1 . 2 . 255

Figure 4–4. Two different Class A IP broadcast addresses

The first address represents a traditional Class A IP broadcast address. The first field of the address is the network address, the second field is the subnet address, and the last two fields are the host address (in this case, broadcast). The Expert analyzer will correctly analyze this frame, using its default Class A subnet mask.

The second address shows a non-traditional Class A IP broadcast address. Instead of limiting the subnet address to the second field, this address uses the second and third fields as the subnet address, and only the fourth field as the host address (still broadcast). Using the default Class A subnet mask, the Expert analyzer would mistakenly interpret the subnet address as 1. The Expert analyzer would fail to register

the broadcast address, and would create a spurious network object for the host address 2.255.

IMPORTANT: It is essential that you enter the IP network address and appropriate subnet mask for the networks from which the Expert analyzer will see frames. Failure to do so can result in false network objects and diagnoses.

The Expert analyzer's configuration function allows you to add, delete, or change user-configured subnet masks. You can also edit or delete the analyzer's default subnet masks.

To add a specific IP network address and associated subnet mask:

1. Move to the **Expert config\Subnet masks** option.
2. Press ENTER. The box in Figure 4–5 appears.

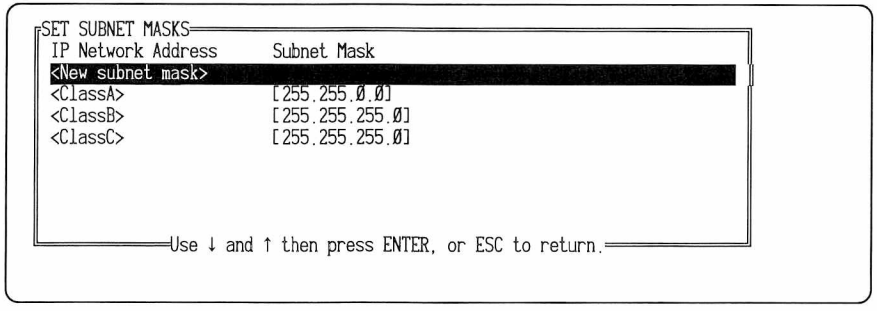


Figure 4–5. Set Subnet Masks box

3. Highlight <New subnet mask>, and press ENTER.

   NOTE: If you have already entered the maximum number of addresses, the analyzer will indicate this. You will need to delete one of the existing addresses first. See the next procedure, on page 4–11.

4. The box in Figure 4–6 appears. Type in the new IP network address in the format [***n.n.n.n***], where each ***n*** is less than 256, and press ENTER.

   NOTE: The brackets are optional. However, if you include one bracket, you must include both.

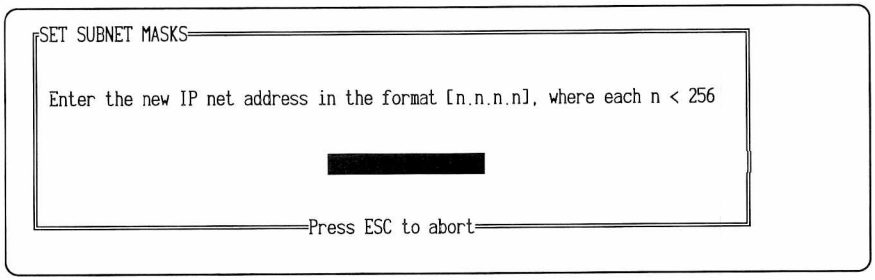


Figure 4–6. Entering the IP network address

5. After you press ENTER, a box (Figure 4–7) appears in which you enter the subnet mask associated with the IP network address you just entered. Enter the subnet mask in the form ***[n.n.n.n]***, and press ENTER.

   NOTE: Depending on the class IP network address you entered, the analyzer may supply the first fields of the subnet mask for you. The analyzer will not allow you to enter an illegal network address/subnet mask pair.

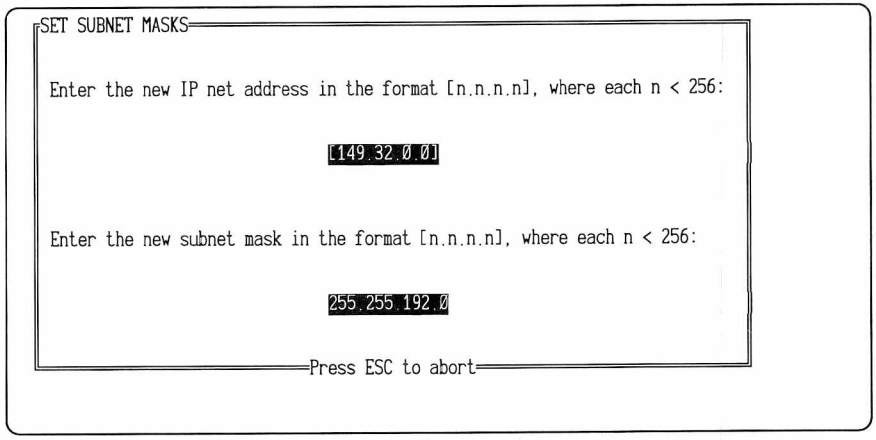

SET SUBNET MASKS
Enter the new IP net address in the format [n.n.n.n], where each n < 256:
[149.32.0.0]
Enter the new subnet mask in the format [n.n.n.n], where each n < 256:
255.255.192.0
Press ESC to abort

Figure 4–7. Entering the associated subnet mask

6. After you have entered the IP network address and subnet mask, the analyzer adds the new entries to the list, as shown in Figure 4–8.

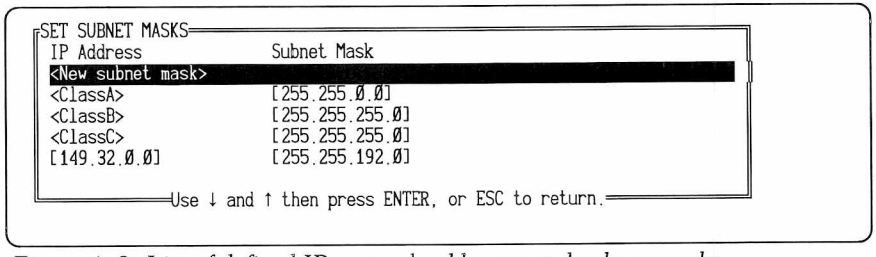


Figure 4–8. List of defined IP network addresses and subnet masks

You can also modify or delete existing IP network addresses and subnet masks.

To modify or delete existing IP network addresses and subnet masks:

1. Move to the **Expert config\Subnet masks** option and press ENTER. The list in Figure 4–5 appears.
2. Highlight the IP network address and associated subnet mask you want to modify or delete and press ENTER.
   The box in Figure 4–9 appears.

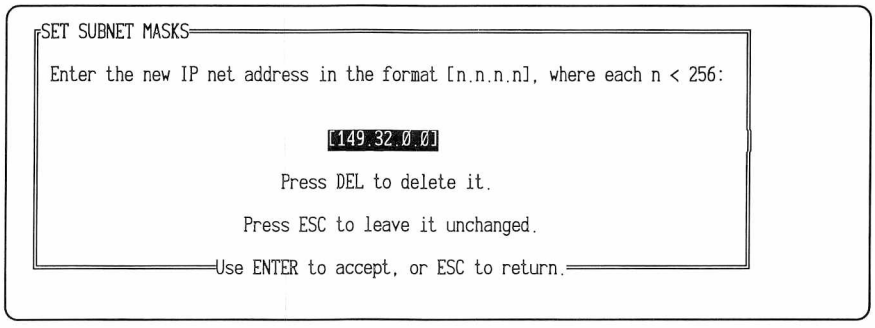

SET SUBNET MASKS
Enter the new IP net address in the format [n.n.n.n], where each n < 256:
[149.32.0.0]
Press DEL to delete it.
Press ESC to leave it unchanged.
Use ENTER to accept, or ESC to return.

Figure 4–9. Modifying or deleting the IP address

3. Do you want to delete this IP network address?
   - If so, press DEL. The analyzer posts a warning box and then deletes both the IP address and the associated subnet mask.
   - If not, either press ESC to return to the Set Subnet Masks box, or modify the IP network address and subnet mask using the cursor keys.
4. Once you have deleted or modified the IP network address and subnet mask pair, the analyzer updates the list in Figure 4–8.

As the Expert analyzer captures TCP/IP frames, it will first check its list of user-configured IP network addresses and subnet masks and try to associate the proper address with the incoming frames. If the analyzer does not find the appropriate address in its list of addresses, it will apply the default subnet mask appropriate to the class of address it is currently analyzing.

IMPORTANT: Changes made by the Expert analyzer configuration function become active immediately. There is no need to restart the application. Additionally, any changes made by the Expert analyzer configuration function are automatically saved to the STARTUP.xxV file when you exit the analyzer. The next time the analyzer starts, it will start with the changes you made intact.

Setting Trustee Names

One of the central functions of the Expert analyzer is its ability to learn symbolic names by extracting information from the packets that pass through its real-time protocol interpreters. The Expert analyzer does this automatically, substituting symbolic names for addresses in the Expert displays as it learns them.

Because the Novell environment often uses trustee names to refer to groups of users during bindery requests, the analyzer may incorrectly substitute a name for a network address. For example, suppose the user Agnes is a member of the trustee group CCMAIL. When Agnes requests access to her CCMAIL, the Novell software will first check the bindery for the trustee name CCMAIL and then check if Agnes is a valid member of this group. During the course of this transaction, the analyzer may associate the trustee name CCMAIL with Agnes' station address.

To prevent inaccurate name-address assignment from happening, you can use the Expert analyzer's configuration function to specify trustee names that will be excluded from the Novell name search.

To specify trustee names to be excluded from the Novell name search:

1. Move to the **Expert config\Trustee names** menu option.
2. Press ENTER. The box in Figure 4–10 appears.

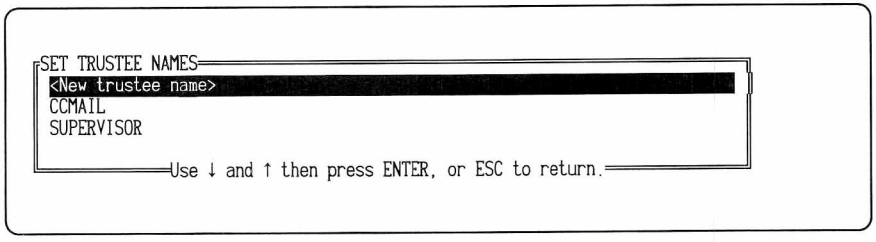


Figure 4–10. Set Trustee Names box

3. Highlight <New trustee name> and press ENTER. The box in Figure 4–11 appears.
   NOTE: If the maximum number of trustee names has already been entered, a pop-up box will inform you of this. You will need to delete an existing trustee name in order to add a new one.

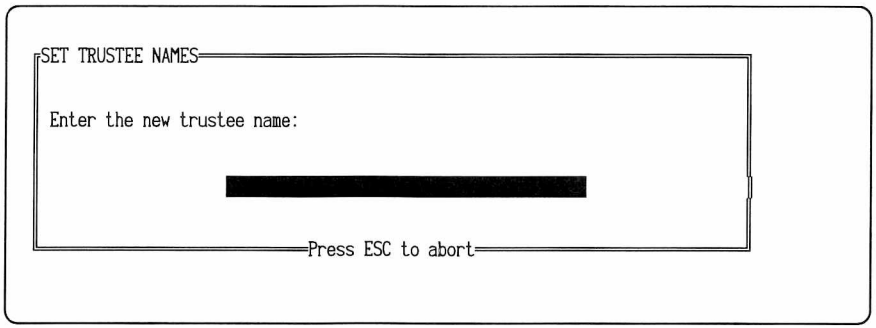


Figure 4–11. Entering a new Trustee Name

4. Enter the trustee name which you want the Expert analyzer to ignore during the Novell name search. The following common names are provided by default:
   - CCMAIL
   - SUPERVISOR
5. Press ENTER. After the name has been entered, it will appear in the Set Trustee Names box in Figure 4–10.

To delete or modify trustee names:

1. Use the procedure above to go to the Set Trustee Names box.
2. In the list that appears, highlight the name you want to modify or delete. Press ENTER.
3. In the box that appears, you can press the DELETE key to delete a trustee name or modify a name using the keyboard.

IMPORTANT: Changes made by the Expert analyzer configuration function become active immediately. There is no need to restart the application. Additionally, any changes made by the Expert analyzer configuration function are automatically saved to the STARTUP.xxV file when you exit the analyzer. The next time the analyzer starts, it will start with the changes you made intact.

Setting Thresholds for Symptoms and Diagnoses

The thresholds in the analyzer's **Expert config\Thresholds** menu determine whether the analyzer generates a symptom or diagnosis message based on a given network event. This section describes how to set the Expert thresholds.

IMPORTANT: The default thresholds supplied with the Expert analyzer have been carefully calculated to ensure accurate and informative symptom and diagnosis detection. Before changing any of the thresholds, make sure you understand:

- How the Expert thresholds interact with one another to determine symptom and diagnosis detection. This section describes each threshold, and the symptoms and diagnoses associated with them.
- Your network. The final responsibility for creating an informative set of Expert thresholds lies with you. You should not change any of the Expert thresholds until you have established a network baseline and are sure the new values are appropriate for your particular network.

  For example, after capturing with the default Expert thresholds you may find that the analyzer is registering repeated **LAN overload** diagnoses. Upon closer examination you find that the amount of traffic on this particular segment was, in fact, quite normal for your particular network. If that is the case, you may want to increase the **LAN overload** threshold to a higher rate of traffic, ensuring that the analyzer reveals a diagnosis only when the amount of traffic on this segment presents a problem.

NOTE: You can always use the **Use defaults** command in the Options menu to reset all the Expert thresholds to their original values. Be aware that the **Use defaults** command will reset all settings in the analyzer's menus to their original values. For more information on using the **Use defaults** command, refer to Chapter 3.

To set an Expert threshold:

1. From the Main Menu, use the cursor keys to move to the **Expert config\Thresholds** menu.
2. Move the highlight to the Expert layer associated with the threshold you want to change.

   The right panel displays a list of thresholds associated with the highlighted layer, as shown for the Connection layer in Figure 4–12.

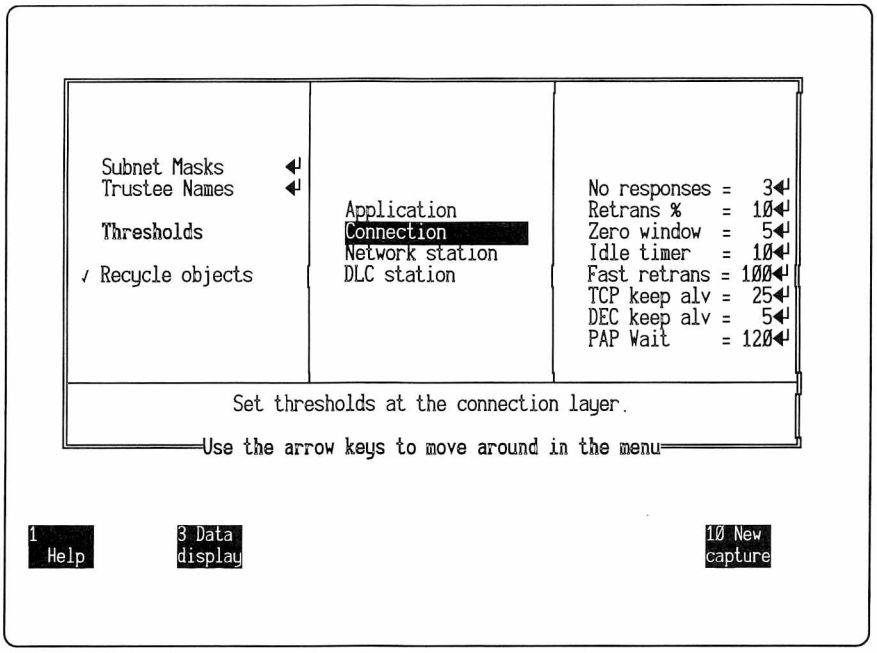


Figure 4–12. The Expert config\Thresholds\Connection layer menu

3. Use the cursor keys to move the highlight to the desired threshold. Press ENTER.
4. Type the new value for the desired threshold in the dialog box that appears and press ENTER.

The newly defined threshold takes effect the next time you do either of the following:

- Start capture in Expert mode
- Display the frames in the capture buffer

IMPORTANT: When you display frames after changing an Expert threshold, the analyzer automatically performs Expert analysis on all frames in the capture buffer, generating symptom and diagnosis messages according to the new Expert thresholds. Previous analysis results are lost. For more information on this concept, see "Effects of Changing Expert Thresholds" on page 4–32.

Symptom and Diagnosis Thresholds at Each Expert Layer

This section describes the meaning of each user-defined Expert threshold and how it affects symptom and diagnosis detection. Depending on the topologies you ordered from the factory, the exact thresholds available on your analyzer may be a subset of those described here. Figure 4–13 shows the available thresholds at each Expert layer. The thresholds are described in the same order in which they appear in the analyzer's menus.

How the Expert Thresholds Interact

Many of the Expert thresholds work in tandem to determine symptom and diagnosis detection. For example, at the Data Link layer, the analyzer displays a symptom message when network traffic exceeds the Expert threshold, **LAN overload** (by default, 30 percent of available bandwidth). In each minute, if network traffic exceeds the **LAN overload** threshold for more than 20 percent of the time (defined by the threshold **LAN overload %**), the analyzer will diagnose that the network is overloaded.

In other words, one threshold (**LAN overload**) specifies when a symptom is detected. The second threshold, usually specified as a percentage (in this case, **LAN overload %**), specifies at what point a symptom becomes problematic enough to be considered a diagnosis. Figure 4–13 indicates pairs of thresholds that work in this manner by displaying them side by side.

Expert Layer	Expert Threshold	Related Expert Threshold
Application Layer	Minimum Application Requests	
	Response Time	Slow Response Percentage
	Filter Time	Denied Count
	Filter Time	Loop Percentage
	Denied Request Percentage	
	Local Transfer/Remote Transfer	Slow File Percentage
Connection Layer	No Responses	
	Retransmission Percentage	
	Zero Window	
	Idle Timer	
	Fast Retransmission	
	TCP Keep Alive	
	DEC Keep Alive	
	PAP Wait	
Network Layer	Multiple Routers	
	DEC Hello	
	Duplicate Percentage	
DLC Station Layer	LAN Overload	LAN Overload Percentage
	Broadcast Symptom	Broadcast Diagnosis
	Physical Errors	
	WAN Overload*	WAN Overload Timer*
	WAN Underload*	WAN Underload Timer*
	Congestion Percentage*	
	ZIP Storm	
MAC Layer (Token Ring)	Ring Entries	
	Receiver Congestion	
	Station Removed	
	Ring Errors	
	Ring Purge Symptom	Ring Purge Diagnosis

Figure 4–13 Expert thresholds available at each Expert layer

Application Thresholds

The Expert thresholds at the Expert Application layer are related to the quality of connections and file transfers. The thresholds are described in the same order as they appear in Figure 4–13.

Minimum Application Requests

The **Min appl req** threshold specifies the minimum number of application requests that must have been sent by a specific application before the analyzer will display an Application layer diagnosis related to that application.

Suppose **Min appl req** is set to 100 (the default). If Station A has sent Station B 25 file requests and a file retransmission occurs, the analyzer will not generate the **File retransmission** diagnosis (or any other diagnosis) because there have not yet been 100 application requests between Station A and Station B. The **Min appl req** threshold helps ensure that the Expert analyzer bases a symptom or diagnosis on reliable statistics, not a few isolated instances of abnormal network activities at the Application layer.

Possible values range from 0 to 999; default value is 100.

Response Time

The threshold **Response time** specifies the time limit within which a Server should respond to an application request. If the Server sends a response after the timer expires, the analyzer considers the response "slow." This threshold alone does not generate a symptom or diagnosis. However, if the ratio of slow responses to normal responses exceeds the threshold set by **Slow resp %**, the analyzer generates the diagnosis **Slow server**.

Response time measures the time (in milliseconds) between when an application request is sent and a response is received.

Possible values range from 0 to 999 milliseconds; default value is 100 milliseconds.

Slow Response Percentage

The **Slow Response Percentage** threshold determines whether the analyzer considers a server slow in responding to application requests. The diagnosis is **Slow server**.

The value is the ratio between slow responses and normal responses in percentage. This percentage is calculated by the following expression:

Number of slow responses / Number of normal responses x 100

A response is considered slow if the response time exceeds the value defined by the threshold **Response time**.

Possible values for the **Response time** % threshold range from 0 to 100 percent; default value is 20 percent.

Filter Time

The **Filter time** threshold specifies (in seconds) the maximum time interval during which the analyzer counts repeated requests and denied requests. Each time an application process sends out a request, the analyzer resets the filter timer. If the same request is sent out again before the filter timer expires, the second request is considered a repeated request. For example, if the **Filter time** threshold is set to five seconds and an application sends out the same request one minute after the first one, the second request is not considered a repeated request.

The **Filter time** threshold also determines whether the analyzer counts a given denied request. For example, some printers poll servers at regular intervals (such as once every five seconds) to find out if there are print jobs in their queues. If there are no print jobs, the printer's request is denied. Because this is a regular occurrence, you should set **Filter time** low enough so that the analyzer will not register normal network activity (a server denying a printer's request) as excessive denied requests. In this example, if **Filter time** were set less than five seconds, the repeated server polls by the printer would not be counted as denied requests.

The **Filter time** threshold by itself does not result in a diagnosis. However, in tandem with the **Loop** % threshold (see below), it does affect when the diagnosis, "Too many loops (***number of loops***) by ***station name*** to ***station name***," appears.

Additionally, in tandem with the **Denied count** and the **Denied request percentage** threshold, the **Filter time** threshold controls when the symptom, "***x*** denied requests," and the diagnosis, "Excessive denied requests," appear.

Possible values for the **Filter time** threshold range from 0 to 999 seconds; default is 1 second.

Denied Count

The **Denied count** threshold specifies the quantity of denied requests for a given application at which the analyzer will generate the symptom "***x*** denied requests." Notice that the analyzer defines denied requests using the **Filter time** threshold. That is, a request is only counted as denied if it is denied within the time range specified by the **Filter time** threshold (see above for details).

For example, suppose the following thresholds were set:

- **Filter time** = 1 second
- **Denied count** = 2

In this case, the analyzer will only count a request as denied if it occurs within one second from the last denied request. Once the analyzer detects more than two denied requests for a given application, it generates the "***x*** denied requests" symptom.

Possible values for the Denied count threshold range from 1 to 100. The default is 2.

Loop Percentage

While the threshold **Filter time** specifies at what point the analyzer considers an application process request to be a repeated request, the threshold **Loop %** specifies at what point the quantity of these repeated requests presents a problem.

The value of **Loop %** is the ratio between repeated requests and normal requests. A repeated request is one that is sent out even though the proper response to the previous request has already been seen by the analyzer. The analyzer does not count certain repeated requests. For example, if a repeated request is sent after the **Filter time** threshold expires, the analyzer "forgets" the previous request and does not consider this one a repeated request. A normal request is any request that is not deemed repeated by the analyzer.

NOTE: Repeated requests exclude the read or write requests involved in file transfers.

The analyzer calculates the value for **Loop %** by the following equation:

Number of Repeated Requests / Number of Normal Requests x 100

The diagnosis is, "Too many loops (***number of loops***) by ***station name*** to ***station name***." The analyzer displays separate diagnosis messages for different connections, even if the connections originate from the same station. For example, if Station A is sending a high number of repeated requests to both Server 1 and Server 2, the following diagnoses appear:

Too many loops (68) by Station A to Server 1
Too many loops (70) by Station A to Server 2

Possible values for the **Loop %** threshold range from 0 to 100 percent; default value is 30 percent.

Denied Request Percentage

The **Denied req %** threshold specifies the maximum acceptable percentage of denied versus successful application requests for a given application. If this percentage is exceeded, the analyzer reveals the diagnosis, **Excessive requests denied from *station name***.

The value for **Denied req** % is calculated as follows:

Number of denied requests / Number of successful requests x 100

Note that the analyzer uses the **Filter time** threshold to determine whether it should consider a request as denied or not. See "Filter Time" on page 4–19.

Possible values range from 0 to 100 percent; the default is 20 percent.

Local Transfer/ Remote Transfer

The **Local Transfer** and **Remote Transfer** thresholds specify the minimum acceptable rate of data transfer for a file transfer between two stations. If the rate of a given file transfer falls below the specified minimum data rate, the analyzer will reveal the symptom **Low Throughput**.

Meaning:

- **Local transfer**– Speed of file transfer between two stations on the same subnetwork. Possible values range from 0 to 999 KBps; default is 170 KBps.
- **Remote transfer**– Speed of file transfer between two stations separated by at least one bridge/router (that is, with a hop count greater than or equal to one). Possible values range from 0 to 999 KBps; default is 50 KBps.

NOTE: Local transfer and **Remote transfer** are separate thresholds. The analyzer applies two different minimum transfer rates depending on whether a given connection is defined as remote or local. Local transfers have hop counts of zero. Remote transfers have hop counts of one or more. Normally, file transfer becomes slower as the hop count increases, so you should set the **Local transfer** threshold to a greater value than **Remote transfer**.

The frequency of slow file transfers between two stations affects when the analyzer displays the diagnosis, **Slow File Transfer**. See the definition for **Slow File Percentage**, below.

Slow File Percentage

The **Slow File Percentage** threshold specifies the maximum percentage of slow file transfers versus normal file transfers for a given connection. If the specified ratio is exceeded, the analyzer diagnoses that the file transfer process between two stations is too slow. The diagnosis is **Slow File Transfer**.

Slow File Percentage is calculated as the ratio between slow file transfers and normal file transfers. Slow file transfers are those whose rates are less than the **Local transfer** or **Remote transfer** thresholds. Normal file transfers are those whose rate exceeds the minimum acceptable data rate specified by the **Local transfer** or **Remote transfer** thresholds. **Slow File Percentage** is calculated by the following equation:

Number of slow file transfers / Number of normal file transfers *x* 100

NOTE: The analyzer will make a diagnosis only after 10 file transfers have taken place.

Possible values range from 0 to 100 percent; default value is 30 percent.

File Overlap/Retransmissions

NOTE: The **Slow file percentage** threshold also specifies the maximum percentage of file retransmissions versus normal file transfers for a given connection. If the specified ratio is exceeded, the analyzer diagnoses that there are too many retransmissions on the connection. The diagnosis is **File overlap/retransmissions.**

Connection Thresholds

The Expert thresholds in this section refer to specific connections detected at the Expert Connection layer. The thresholds are organized in the same order they are found in the **Expert config\Thresholds\Connection** menu.

No Responses

The **No Responses** threshold specifies the number of consecutive retransmissions in the same direction on a single connection without response that implies a connection is broken. For example, if **No responses** has been set to 3 (the default), the analyzer will diagnose that a connection is lost after a packet has been retransmitted 3 times. The analyzer will generate both a diagnosis and a symptom message. The message is **Non-responsive station:** ***Station name***.

Possible values range from 0 to 999; default value is 3.

Retransmission Percentage

The **Retransmission Percentage** threshold specifies the maximum acceptable percentage of retransmitted packets versus successfully transmitted packets in the same direction on a single connection at the Connection layer. If this percentage is exceeded, the analyzer generates the diagnosis **Retransmissions**. The value for **Retrans %** is calculated as follows:

Number of retransmitted packets / Number of non-retransmitted packets x 100

Possible values range from 0 to 100 percent; default value is 10 percent.

Zero Window

The **Zero Window** threshold specifies the duration of a zero window before the analyzer displays the symptom message, **Zero window for** ***x*** **seconds**. A network

station receiving data notifies the sender of its buffer size (the window size). A zero window indicates that the receiver's buffer is full. Transmission to this station stops until it sends a non-zero window advertisement.

The threshold value is the time between a zero window advertisement and the subsequent non-zero window advertisement.

Possible values range from 0 to 999 seconds; default is 5 seconds.

Idle Timer

The **Idle Timer** threshold specifies in minutes the maximum time a connection at the Expert Connection layer can remain idle. A connection is considered idle if no packets are sent in either direction. If the idle time of a given connection exceeds the **Idle Timer** value, the analyzer generates the symptom **Idle more than *x* minutes**.

Possible values range from 0 to 999 minutes; default value is 10 minutes.

Fast Retransmission

The **Fast Retransmission** threshold specifies the minimum time between packet retransmissions. If a station retransmits a packet before the analyzer's **Fast retrans** timer has expired, the analyzer generates the symptom **Retransmission with too short timer**.

Possible values range from 0 to 999 milliseconds; default value is 100 milliseconds.

TCP Keep Alive

The **TCP Keep Alive** threshold is used to specify whether a retransmitted frame represents a real retransmission or a "keep alive" frame. For example, if **TCP keep alv** is set to 10 seconds, a frame retransmitted more than 10 seconds after its first transmission is considered a TCP keep alive.

Possible values range from 0 to 999 seconds; default is 25 seconds.

DEC Keep Alive

The **DEC Keep Alive** threshold is used to specify whether a retransmitted frame represents a real retransmission or a "keep alive" frame. For example, if **DEC keep alv** is set to 10 seconds, a frame retransmitted more than 10 seconds after its first transmission is considered a DEC keep alive.

Possible values range from 0 to 999 seconds; default is 5 seconds.

PAP Wait

The **PAP Wait** threshold determines how long a user on an AppleTalk connection can wait for a printer, before the analyzer will generate the symptom **Excessive wait for printer**.

Possible values range from 1to 999 seconds; default is 120 seconds.

Network Station Thresholds

The Expert thresholds in this section refer to symptoms and diagnoses at the Network layer. Symptoms and diagnoses at the Network layer are associated with network addressing and routing problems. The thresholds are organized as they are found in the **Expert config\Thresholds\Network Station** menu.

Multiple Routers

The **Multiple Routers** threshold specifies the maximum number of local routers through which local traffic can be routed to a remote station. If there are more routers than specified, the analyzer displays the diagnosis **Multiple routers to station *station name***.

Possible values range from 0 to 10; default is 3.

DEC Hello

If the DECnet hello timer is less than the value specified for **DEC hello**, the analyzer will trigger the symptom **Small hello time**.

DECnet uses hello packets for neighbor identification. In a DECnet environment, a station needs to know of at least one intermediate system (a router) to which it can hand off packets with unknown destinations. Hello packets let a station find this default intermediate system. The DECnet hello timer controls how often hello packets are sent. Because hello packets contribute to network overhead, the hello timer should be set as high as possible, depending on the stability of the environment. A short hello timer can lead to high network traffic and routing problems.

Possible values range from 0 to 999 seconds; default is 10 seconds.

Duplicate Percentage

The Expert analyzer uses several different algorithms to detect the presence of duplicate network addresses on the network. The **Duplicate address percentage** threshold allows you to fine-tune the algorithm specific to the DECnet environment.

In the DECnet environment, stations are required to send a hello packet at a specified time interval (for an explanation of the DEC Hello packet, see, "DEC Hello," above). The analyzer uses these hello packets to detect duplicate network addresses. Because the time between hello packets for a given station should theoretically remain a constant, the analyzer will generate a **Duplicate net address** diagnosis if it detects a discrepancy in the intervals for hello packets sent from a single network address. Because of fluctuations in the intervals of hello packets with the same network address, the analyzer assumes that two different stations are sending hello packets with the same network address.

Theoretically, the interval between hello packets for a given network station should remain constant. However, due to various network irregularities, the interval tends to vary within a small range of the specified interval. As capture proceeds, the analyzer "learns" the usual interval for hello packets from a given station. The **Duplicate address percentage** threshold specifies the maximum percentage discrepancy between the usual DEC hello interval as learned by the analyzer and the measured DEC hello interval of a given frame. Figure 4–14 illustrates the concept of the **Duplicate address percentage** threshold.

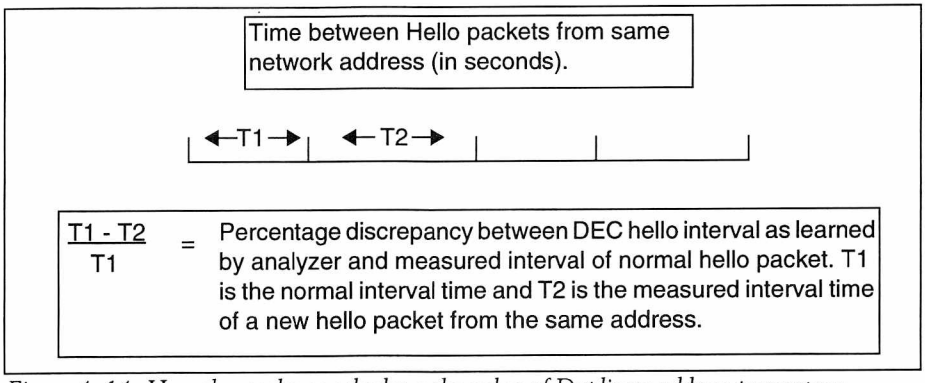

Time between Hello packets from same network address (in seconds).
←T1→
←T2→
T1 - T2 / T1 = Percentage discrepancy between DEC hello interval as learned by analyzer and measured interval of normal hello packet. T1 is the normal interval time and T2 is the measured interval time of a new hello packet from the same address.

Figure 4–14. How the analyzer calculates the value of Duplicate address percentage

If your network is very busy, or has a lot of "noise," you may want to set the Duplicate address percentage threshold at a high percentage to avoid spurious **Duplicate Network Address** diagnoses. Possible values range from 0 to 100 percent; the default is 10 percent.

DLC Station Thresholds

This section describes the Expert thresholds related to symptoms and diagnoses detected at the Expert Data Link layer. Symptoms and diagnoses at the Data Link layer are associated with problems such as broadcast storms and traffic bursts. The thresholds are organized as they are found in the **Expert config\Thresholds\DLC Station** menu. Token ring-specific (MAC level) thresholds are described starting on

page 4–27. WAN/Synchronous-specific thresholds are described starting on page 4–30.

LAN Overload

The **LAN Overload** threshold specifies the network load at which the analyzer should generate a **Network overload** symptom. Network load is measured as a percentage of maximum bandwidth.

Possible values range from 1 to 100 percent; default is 30 percent for Ethernet and 60 percent for token ring.

IMPORTANT: Because of the token-passing nature of token ring networks, collisions are nonexistent. Network loads can therefore remain trouble-free at higher volumes on token ring than on Ethernet. This explains the difference in default values for the **Network overload** threshold.

LAN Overload Percentage

The **LAN Overload Percentage** threshold specifies at what point the analyzer diagnoses that the network is overloaded. The diagnosis is **Overloaded network**.

LAN overload % is measured as the percentage of each minute the network is in overload mode. Whether the network is considered to be in overload mode depends on the setting of **LAN overload**.

Figure 4–15 illustrates the relationship between **LAN overload** and **LAN overload** %. In this example, the threshold **LAN overload** is defined as traffic greater than 30 percent of maximum bandwidth, and the threshold **LAN overload** % is defined as 20 percent. The total number of seconds during which the network experiences an overload is about 20. That is, the network is in overload mode for 30 percent of the time during this minute, which is higher than the **LAN overload percentage** threshold (20 percent). The analyzer diagnoses that the network is overloaded.

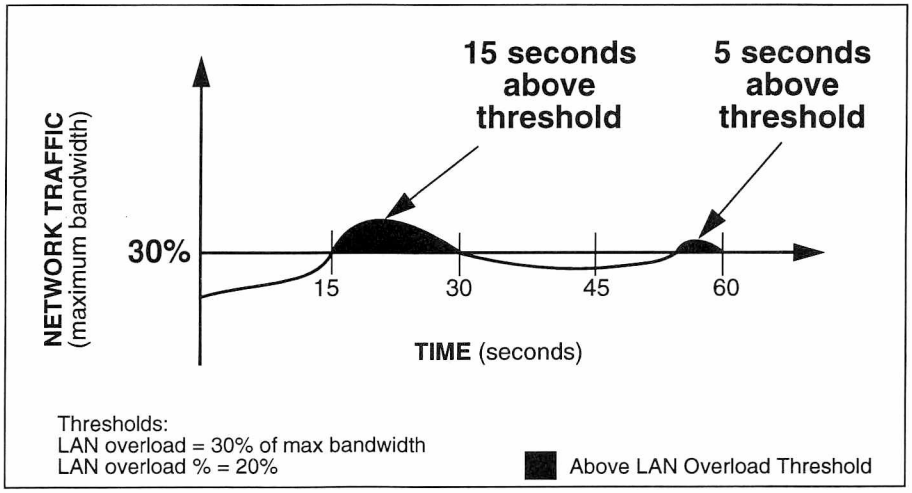


Figure 4–15. The relation between thresholds ***LAN overload*** *and* ***LAN overload%***

Broadcast Symptom

The **Broadcast Symptom** threshold specifies the rate of broadcast/multicast packets per second above which the analyzer will generate the symptom **Broadcast/Multicast storm.**

Possible values range from 0 to 999; default value is 40 broadcast packets per second.

Broadcast Diagnosis

The **Broadcast Diagnosis** threshold specifies the rate of broadcast/multicast packets per second above which the analyzer will generate the diagnosis **Broadcast storm.**

Characteristically, the value that triggers a broadcast storm *diagnosis* (**Broadcast dg**) will be greater than that chosen to trigger a broadcast storm *symptom* (**Broadcast sy**).

Possible values range from 0 to 999; default value is 120 broadcast packets per second.

ZIP Storm

The **ZIP storm** threshold determines how many AppleTalk ZIP Query frames can occur in a one minute interval, before the analyzer will generate the symptom **ZIP storm.**

Possible values range from 1to 999; default value is 10 ZIP Query frames per minute.

Physical Errors

The **Physical Errors** threshold specifies the maximum acceptable number of physical errors per second per station.

If the number of frames with physical errors sent by a given station exceeds the threshold, the analyzer generates the diagnosis **High rate of physical errors by *station name***.

NOTE: The analyzer also tracks the number of physical error frames received by each station. However, this quantity does not affect when the **High rate of physical level errors** diagnosis is generated.

Possible values are 0 to 999 errors per second; default value is 4 errors per second per station.

Token Ring-Specific (MAC layer) Thresholds

This section describes Expert thresholds that are specific to token ring; particularly, thresholds relating to the MAC level. The Expert analyzer captures and decodes all MAC layer (including Report Soft Error) frames on the ring, providing accurate detection of token ring symptoms and diagnoses.

The thresholds are organized in the same order they are found in the **Expert config\Thresholds\DLC Station** menu.

Ring Entries

The **Ring Entries** threshold specifies the rate of ring entries per minute per station at which the analyzer will generate the **High rate of ring entries** diagnosis. For example, if **Ring entries** is set to 2 (the default), the analyzer will generate the diagnosis when the rate of ring entries for a particular station equals or exceeds two per minute.

A station inserting to a ring physically "breaks" the ring as its relay in the multistation access unit (MAU) opens and the lobe becomes part of the ring. The ring recovers quickly, as this is normal token ring behavior. However, it is abnormal if there is more than one ring entry per minute for a given station. Default values are set accordingly.

Possible values are 0 to 999 ring entries per minute; default value is 2 per minute.

RX Congestion (Receiver Congestion)

The **RX Congestion** threshold specifies the rate of receiver congestion errors per minute per station at which the analyzer will generate the **High rate of receiver congestion** diagnosis. For example, if **RX congestion** is set to 60 (the default), the analyzer will generate the diagnosis when the rate of receiver congestion errors for a particular station equals or exceeds 60 per minute.

Receiver congestion errors indicate that a station detected a frame on the ring with its own destination address but was unable to copy it because it had no buffer space available. A new receiver congestion error is generated each time a new frame is rejected. Receiver congestion errors can be important guides when judging the adequacy of current servers and gateways on the ring. An abundance of receiver congestion errors from an interconnecting device may point to its obsolescence.

Possible values are 0 to 999 receiver congestion errors per minute. Default is 60 receiver congestion errors per minute.

Station Removed

The **Station Removed** threshold specifies the rate of Station Remove Requests per minute at which the analyzer will generate the diagnosis **High rate of remove from ring requests.** For example, if Station Remove is set to 1 (the default), the analyzer will generate the diagnosis when the rate of Station Remove Requests detected by the analyzer exceeds one per minute.

NOTE: The **Station Removed** diagnosis is not related to the **Station Off Ring** symptom. (For more information on **Station Removed** and **Station Off Ring**, see Appendix A: Symptom and Diagnosis Messages.)

Station Remove Requests are sent by the Configuration Report Server, a virtual entity responsible for the overall health of the ring.

Possible values are 1 to 999 requests per minute. Default is 1 request per minute.

Ring Errors

The **Ring Errors** threshold specifies the rate of ring errors per minute per station at which the analyzer will generate the diagnosis **High rate of line/burst errors**. The threshold specifies the total of both line errors and burst errors per minute. For example, if **Ring errors** was set to three, the analyzer would generate the **High rate of line/burst errors** diagnosis when the rate of total line and burst errors for a given station exceeded three per minute.

Possible values are from 0 to 999 ring errors per minute. Default is 1 ring error per minute.

Ring Purge Symptom

The **Ring Purge Symptom** threshold specifies the rate of ring purges per station per minute at which the analyzer will generate the symptom **High rate of ring purges.** Ring purge frames are sent by the active monitor when it detects that a token has been lost, and are part of normal token ring behavior. However, an excessive amount of ring purge frames on the network can indicate potential hardware problems.

Possible values are from 0 to 999 ring purge frames per minute. Default is 30 ring purge frames per minute.

NOTE: When the **Ring purge sy** threshold is exceeded, the analyzer generates a *symptom*. The analyzer generates a *diagnosis* when the **Ring purge dg** threshold is exceeded. See below.

Ring Purge Diagnosis

The **Ring Purge Diagnosis** threshold specifies the rate of ring purges per station per minute at which the analyzer will generate the diagnosis **High rate of ring purges**. For a brief description of ring purge frames, see, "Ring Purge Symptom," above.

IMPORTANT: Characteristically, the value chosen to trigger a **High rate of ring purges** *diagnosis* **(Ring purge dg)** will be greater than that chosen to trigger a **High rate of ring purges** *symptom* **(Ring purge sy)**.

Possible values are from 0 to 999 ring purge frames per minute. Default is 60 ring purge frames per minute.

WAN/Synchronous (Sniffer Internetwork Analyzer) Thresholds

This section describes those Expert thresholds that are specific to the Sniffer Internetwork Analyzer (that is, the Sniffer analyzer for WAN/Synchronous).

The thresholds are organized in the same order they are found in the **Expert config\Thresholds\DLC station** menu.

WAN Overload

The **WAN Overload** threshold works in tandem with the **Overload Timer** threshold to specify the point at which the analyzer generates the **Network Overload** symptom and the **Overloaded Network** diagnosis.

The **WAN Overload** threshold specifies whether the Expert analyzer considers the network to be in an overload condition. The Expert analyzer considers the network to be in an overload condition if both the DTE and DCE network loads are in excess of the load specified by the **WAN Overload** threshold. The Expert analyzer will continue to consider the network to be in an overload condition until either the DTE or DCE network load falls below the load specified by the **WAN Overload** threshold.

When the duration (in consecutive seconds) of the overload condition exceeds the time specified by **Overload Timer** (below), the analyzer will generate the **Network Overload** symptom (in the Global Symptoms view) and the **Overloaded Network** diagnosis.

Possible values range from 1 to 100 percent; default is 80 percent.

Overload Timer

The **Overload Timer** threshold works in tandem with the **WAN Overload** threshold to specify the point at which the analyzer diagnoses that the WAN is overloaded. The diagnosis is **Overloaded Network**.

The **Overload Timer** threshold specifies the duration (in seconds) of a WAN Overload condition at which the Expert analyzer will generate an **Overloaded Network** diagnosis. Whether the network is considered to be in an overload condition depends on the setting of the **WAN Overload** threshold.

Possible values range from 1 to 999 seconds; default is 60 seconds.

WAN Underload

The **WAN Underload** threshold works in tandem with the **Underload Timer** threshold to specify the point at which the analyzer generates the **Network Underload** symptom and the **Underloaded Network** diagnosis.

The **WAN Underload** threshold specifies whether the Expert analyzer considers the network to be in an underload condition. The Expert analyzer considers the network to be in an underload condition if both the DTE and DCE network loads are below the load specified by the **WAN Underload** threshold. The Expert analyzer will continue to consider the network to be in an underload condition until either the DTE or DCE network load increases above the load specified by the **WAN Underload** threshold.

When the duration (in consecutive minutes) of the underload condition exceeds the time specified by **Underload Timer** (below), the analyzer will generate the **Network Underload** symptom (in the Global Symptoms view) and the **Underloaded Network** diagnosis.

Possible values range from 0 to 100 percent; default is 10 percent.

Underload Timer

The **Underload Timer** threshold works in tandem with the **WAN Underload** threshold to specify the point at which the analyzer diagnoses that the WAN is underloaded. The diagnosis is **Underloaded Network**.

The **Underload Timer** threshold specifies the duration (in minutes) of a WAN Underload condition at which the Expert analyzer will generate an **Underloaded WAN** diagnosis. The setting of **WAN Underload** determines whether or not the network is considered to be in an underload condition.

Possible values range from 1 to 999 minutes; default is 5 minutes.

Congestion Percentage

The **Congestion Percentage** threshold specifies the point at which the analyzer will generate congestion-related symptoms. The **Congestion Percentage** threshold is calculated differently depending on the type of access protocol used by the WAN link to which the analyzer is attached.

Frame Relay

There are two Frame Relay congestion symptoms:

- **Excessive Forward Congestion.** The Expert analyzer generates this symptom when the percentage of forward explicit congestion notification (FECN) frames to total frames on the link exceeds the percentage specified by the **Congestion Percentage** threshold.
- **Excessive Backward Congestion.** The Expert analyzer generates this symptom when the percentage of backward explicit congestion notification (BECN) frames to total frames on the link exceeds the percentage specified by the **Congestion Percentage** threshold.

HDLC

On an HDLC link, the Expert analyzer generates the **Overcongested WAN** symptom when the percentage of receiver not ready (RNR) frames to RNR+Receiver Ready (RR) frames exceeds the **Congestion Percentage** threshold.

Possible values range from 0 to 100 percent; default is 10 percent.

Effects of Changing Expert Thresholds

When you display frames after changing any of the Expert thresholds, the analyzer automatically reanalyzes the frames in the capture buffer. During analysis, the Expert analyzer uses the new Expert settings to generate symptom and diagnosis messages.

WARNING. When the Expert reanalyzes the frames in the capture buffer, it releases all the network objects it has created, including those gleaned from frames no longer in the capture buffer. The results of post-capture Expert analysis will be based solely on information found in the frames currently in the capture buffer. Once network objects associated with frames outside of the capture buffer have been released, they cannot be regained.

Changing the Expert settings will most likely change the results of Expert analysis on a given set of network data. There are at least two ways changing an Expert threshold will affect the results of Expert analysis:

- A modified threshold does not affect the captured data, but the analysis results change because previously analyzed frames are no longer in the capture buffer.
- A modified threshold is relevant to the data currently in the capture buffer. If this is the case, lowering the Expert thresholds will generally increase the number of symptom or diagnosis messages.

The examples below illustrate each of these possibilities.

Example One: Changing a Threshold Irrelevant to the Data in the Capture Buffer

Figure 4–16 illustrates the effect reanalyzing a subset of the frames that have passed through the capture buffer can have on the results of Expert analysis. In this example, the **Physical errors** threshold was set to two for both the original capture session as well as the post-capture analysis. During the original capture session, the analyzer generates the **Physical error** diagnosis when the threshold is exceeded. However, during post-capture analysis, a frame exhibiting one of the physical errors is now outside of the capture buffer. Because the analyzer no longer knows of the existence of that frame, the threshold is not exceeded, and no diagnosis is generated.

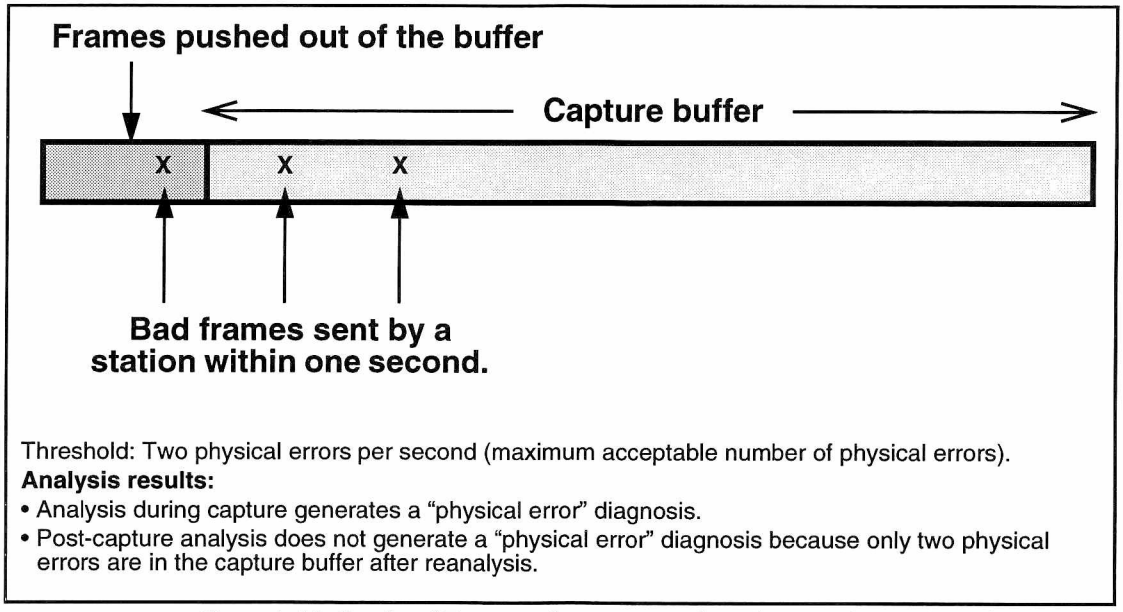

Frames pushed out of the buffer
Capture buffer
X
X
X
Bad frames sent by a station within one second.
Threshold: Two physical errors per second (maximum acceptable number of physical errors).
Analysis results:
• Analysis during capture generates a "physical error" diagnosis.
• Post-capture analysis does not generate a "physical error" diagnosis because only two physical errors are in the capture buffer after reanalysis.

Figure 4–16. Results of Expert analysis can vary depending on when performed

Example Two: Changing a Threshold Relevant to the Data in the Capture Buffer

In some cases, the effect of a modified Expert threshold is not as obvious. Consider the following example:

You are capturing frames from a trace file and analyzing with the data link threshold settings as follows:

- **LAN overload** = 30% (percentage of available bandwidth)
- **LAN overload %** = 20
- **Broadcast sy** = 2
- **Broadcast dg** = 1
- **Physical err** = 4

Under these data link thresholds, the analyzer detects a broadcast storm symptom after capturing frame 38 at 16:18:14.3693.

Suppose you capture again from the same file with this new threshold setting:

- **LAN overload**= 8%

Although the thresholds related to broadcast storms remain unchanged, the new analysis results show no broadcast storm symptoms or diagnoses. Instead, the analyzer detects a Network overload symptom at 16:18:13.7949.

What happened? With the decreased threshold for **LAN overload**, it became much easier to trigger a Network overload symptom. Frame 38 captured at 16:18:13.7949 exceeded the new threshold for **LAN overload**, and the analyzer alerted us to a LAN overload symptom. The analyzer never realized that Frame 38 also exceeded the **Broadcast sy** threshold. Because the analyzer stops analyzing a frame after detecting the first symptom or diagnosis associated with a frame, it is possible that a frame has more than one symptom, and the analyzer only displays a message for the first symptom or diagnosis detected.

Figure 4–17 illustrates the time passage between the detection of the two symptoms.

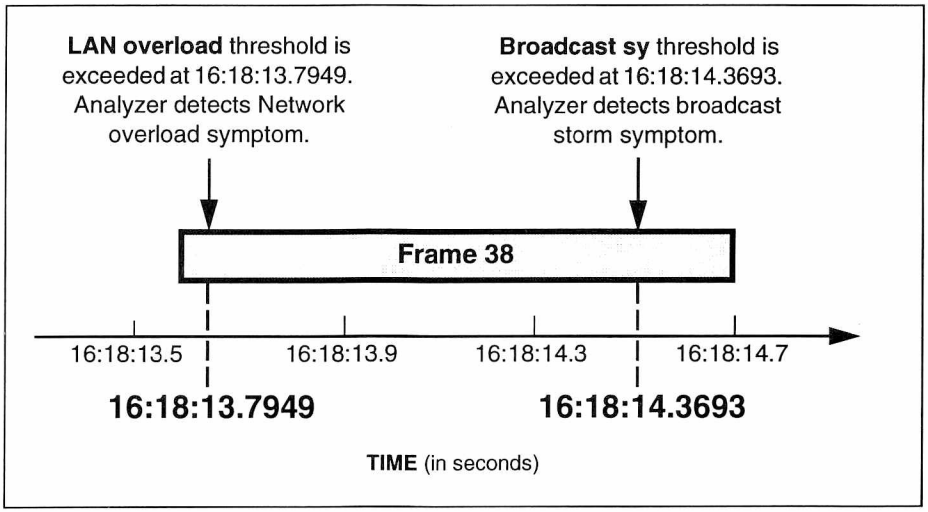


Figure 4–17. A single frame with two symptoms. Only the first is detected by the analyzer.

Customizing a Capture Session

You can customize an Expert capture session by specifying the screen format, capture filters, frame size, and so on. In addition, there are several Expert-specific options which allow you to further customize a capture session. This section describes the following menu options:

- **Recycle objects** — Specifies whether the Expert analyzer should reuse its memory when there is no more room for new network objects.
- **Name Width** — Allows you to specify the width (in characters) allotted to names in Expert displays.

Each of these options is described below.

Recycle Objects Option

As the Expert analyzer captures frames from the network, it uses the information in those frames to build a database of network objects. Because some networks can be

immensely complex in their structure, at some point the Expert analyzer will have no more memory for new network objects in its database. The checkmark option, **Recycle objects,** allows you to specify what action the analyzer should take when it runs out of memory for new network objects.

You can choose either to recycle objects or not to by highlighting the **Expert config\Recycle objects** option and pressing Spacebar. The options are mutually exclusive. Effects are summarized below:

- **No recycling** — The analyzer will create no more new objects, but will instead continue to interpret network traffic in accordance with the information it has already stored in its database. Symptoms and diagnoses will be revealed according to the information already in the Expert analyzer's database.

- **Recycle objects** — The analyzer will continue to add new objects to its database, overwriting those objects that are least interesting. This is the default. See "How the Expert Analyzer Reuses Network Objects," below.

How the Expert Analyzer Reuses Network Objects

When the Expert analyzer reuses the memory associated with less interesting network objects, it does so via a "smart" algorithm that, in effect, allows it to "forget" outdated network information. The list below summarizes the types of network objects the analyzer will and will not reuse:

The analyzer will **not** reuse:

- Network objects that have symptoms or diagnoses associated with them
- A network object currently highlighted in the Expert window

The analyzer will reuse:

- Network objects with ten or less associated frames and no associated errors

For example, the Expert analyzer will create objects in its database for network stations that have never transmitted or received a frame. Various routing protocols, such as the Routing Information Protocol (RIP), require regular route advertisements showing which stations can be accessed by a given router. The Expert analyzer can learn about non-transmitting stations from such route advertisements. When **Recycle objects** is selected, the Expert analyzer will reuse objects associated with non-transmitting stations like these and replace them with new information.

Name Width Display Option

You can define the width of the name field in the Expert summary and detail displays, from 6 characters up to 31 characters (the default is 15 characters). For example, if the Expert analyzer discovers many large names, you may want to make the name field wider to accommodate the names.

Once you've increased the name width, other information fields may be partially hidden beyond the right limit of the display. That information is still there; you simply need to scroll to reach it. The Expert analyzer allows you to use the cursor keys to scroll horizontally and read information temporarily "hidden" at the edge of the display.

If the display includes a name longer than the specified name width, the Sniffer analyzer truncates that name and replaces its last two visible characters with dots (to show that the name has been truncated). For example, if the **Name width** option specifies an 8-character field and the analyzer discovers the 10-character name **"FileServer,"** the Summary view would show **"FileSe . . "**

To define the Name width option:

1. Move to **Name width=** and press ENTER.

   The **Name width** command is available in three places in the Sniffer analyzer menus:

   - In the **Capture\Screen Format\Expert window** menu.
   - In the **Display** menu.
   - From the **Display Options** menu. The **Display Options** menu is available by pressing F6 **[Disply options]** during post-capture display.

   All three locations are linked. If you change the name width in one location, it is automatically synchronized throughout the menus.

2. In the dialog box that appears, enter the desired name width.

   NOTE: The width you specify in this dialog box will apply to both the Expert and Classic summary and detail displays.

How the Expert Analyzer Learns Symbolic Names

During capture, the Expert analyzer uses its real-time protocol interpreters to learn about the symbolic names for the various network stations, servers, routers, and other network stations. The Expert analyzer can rapidly decode the frames it captures, associating the symbolic names it finds with the related network stations. As the analyzer learns names, it will substitute the symbolic names for the hex or IP addresses in the Expert displays.

Some network protocols have a command that lists all users currently logged on to a given file server. When this occurs, the Expert analyzer captures the relevant packets and extracts all the names from that packet, associating them with the appropriate network address. The following procedure shows how to use this "trick" to help the analyzer learn names almost instantly.

To help the Expert analyzer learn symbolic names:

1. From a workstation the Sniffer Network Analyzer can "see", type the following command:

   -If Novell:

   ```
   USERLIST /A
   ```

   -If TCP/IP running Sun Network Information Services (also known as Sun Yellow Pages).

   ```
   YPCAT HOSTS.BYNAME
   ```

2. Once the Expert analyzer captures the relevant packets, it will substitute the symbolic names it has learned for the addresses in the Expert displays.
3. At the end of the capture session, you may want to use the **Save names** option to save all of the names the Expert analyzer has learned to the name table. For more information on the **Save names** option and how the analyzer works with the name table, see the *Expert Sniffer Network Analyzer Operations manual.*

NOTE: The Expert analyzer still "knows" the actual address of each station. That information is available in the Detail window. See Chapter 5 for more information on the Detail window.

NOTE: In a Novell environment, this trick only works for those stations which are currently logged on to the file server to which the request is made. For example, if WorkStation A is logged on to the file server BIZ-ONE and makes a `USERLIST /A` request, the analyzer will only learn the symbolic names of those stations currently logged on to BIZ-ONE.

Expert Analyzer Capture and Display

5

Expert Analyzer Capture and Display

Overview

You can display the results of Expert analysis at many different levels of detail. This chapter describes the various displays containing the results of Expert analysis. The chapter is organized as follows:

- Explanation: navigating through the Expert displays.
- Description of the Global Statistics display.
- Descriptions of the various Diagnosis displays.
- Descriptions of the various Symptom and Network Object displays.

The chapter also discusses traversing the various Expert displays to get the maximum amount of information on a network problem or connection.

All the Expert screen displays available during capture are also available during post-capture display. You can use the Expert window for display just as you would to capture.

Displaying Analysis Results In the Expert Window

When you start capture in Expert mode, the analyzer automatically sets the screen format to the Expert window. By default, the analyzer displays the Expert Overview. The Expert Overview provides your "home base" for tracking and investigating network problems detected by the analyzer. The Expert Overview tabulates all detected network objects, symptoms, and diagnoses, organizing them by the Expert layer at which they occur. You can use the cursor keys to highlight the various fields in the Expert Overview and press ENTER to view more detailed screens.

Figure 5–1 summarizes the various displays available in the Expert window.

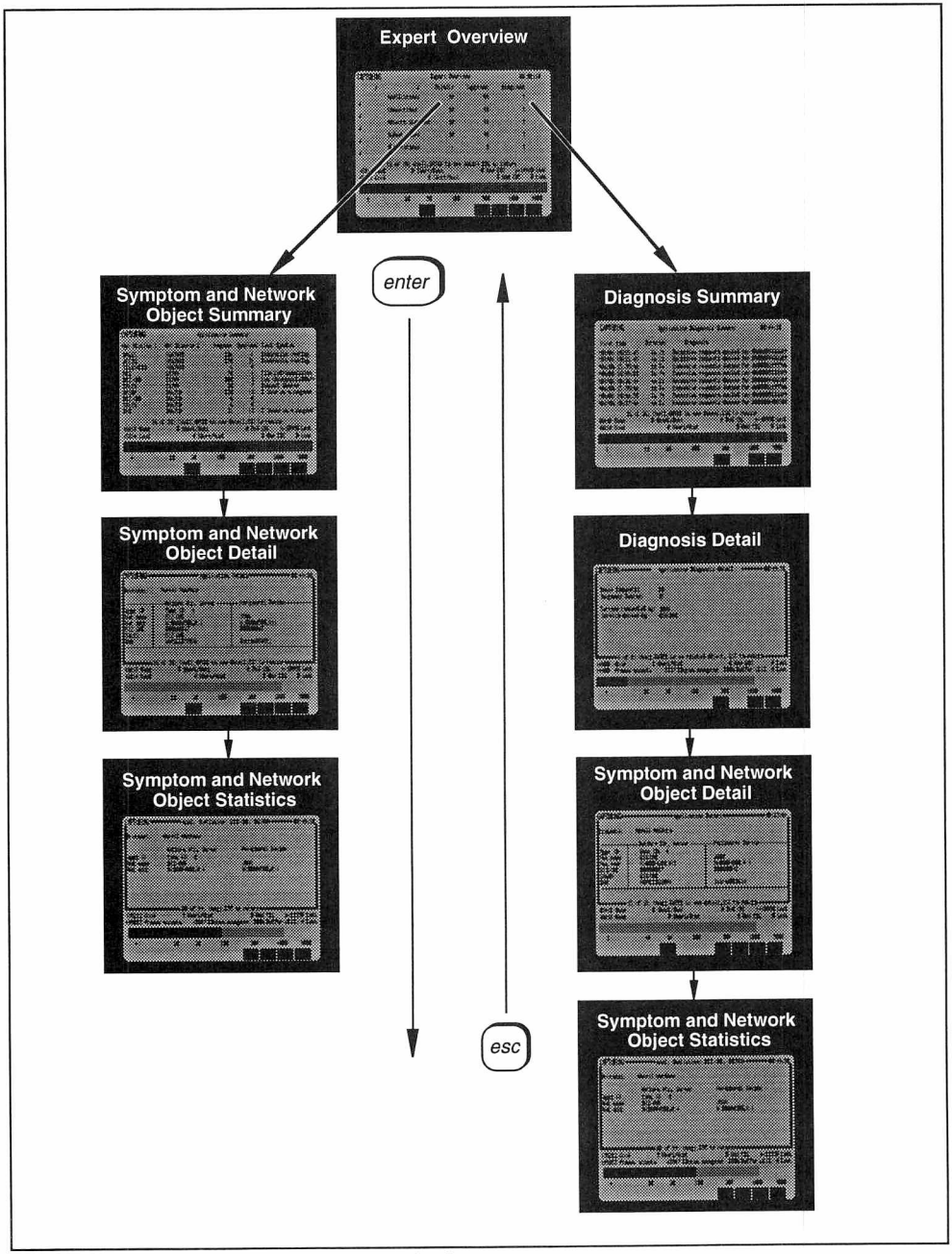


Figure 5–1. Expert analyzer displays

While the Expert displays begin with the Expert Overview, subsequent displays are divided between two categories:

- Diagnosis-related displays
- Symptom and Network Object-related displays

Although the various displays in these two categories are similar in content, their purposes are different. The diagnosis-related displays allow you to track network problems that demand immediate attention. The symptom and network object displays provide you with a barometer of the overall health of your network. Typically, the quantity of symptoms on a given network will greatly exceed the number of diagnoses.

Expert analysis results can be displayed at four levels of detail—overview, summary, detail, or statistics displays. The list that follows briefly describes the contents of each display.

Overview

The Expert Overview provides a summary of all information detected by the Expert analyzer. The Expert Overview tabulates the number of network objects, symptoms, and diagnoses detected at each Expert layer, in addition to a one-line summary of some critical diagnoses.

It may be helpful to think of the Expert Overview as a "home base" from which you can go to the Expert analyzer submenus. By highlighting the fields in the Expert Overview and pressing ENTER, you can get more detailed information about specific network problems detected by the Expert analyzer.

Summary

The Diagnosis Summary window contains a list of all diagnoses detected at the selected layer. This list contains brief descriptions of the detected diagnoses and when they occurred.

Symptom and Network Object Summary windows list all network objects detected at the selected layer and a description of the last symptom (if any) associated with each network object.

Detail

Diagnosis Detail displays show specific information about a particular diagnosis. The information in this view is designed to help you solve the network problem indicated by the diagnosis. Information in this display could include the addresses of the most active stations during a traffic burst, the address of a slow server, or the name of a non-responsive station. The exact information depends on the particular diagnosis. The various Diagnosis Detail displays are described starting on page 5–14.

Symptom and Network Object Detail windows show detailed information about the highlighted network object and any symptoms associated with that object. This information could include the addresses of all stations connected to a selected server, the average packet length of frames on a particular connection, and so on. The exact information depends on the Expert layer and the highlighted network object. Symptom and Network Object Detail windows are described starting on page 5–52.

Statistics

Statistics displays provide specific information about a particular connection or network station. The information in this view could include total bytes transferred on a connection, average frame length, average file performance and number of broadcast frames sent. The exact information depends on the Expert layer selected. Statistics displays are described starting on page 5–60.

The Expert Analyzer also has a Global Statistics view. The Global Statistics view provides a percentage breakdown by protocol family of all detected network traffic. Additionally, the Global Statistics view provides information on bandwidth utilization and general information about the current capture session. The Global Statistics window is described starting on page 5–72.

Each of these displays is described further in later sections.

Navigating the Expert Window

You can always navigate the various Expert displays using these methods:

- To move from a general to specific display, highlight a field that interests you and press ENTER. (Use CURSOR UP, CURSOR DOWN, PGUP, PGDN, HOME, and END to move the highlight.) For example, in the Expert Overview, you can highlight the Diagnoses field at the Application layer and press ENTER to display a list of diagnoses detected at the Application layer.

- To move from a specific to a general display, press ESC.
- If the width allotted to names in the Expert displays has been expanded with the **Name width** command, there may be some information out of sight at the right edge of the Summary displays. The analyzer will indicate this by replacing the last two visible characters with periods. (For example, "Fileserver" might become "Fileserv..")You can use the cursor keys to scroll horizontally until the hidden information becomes visible. Horizontal scrolling is available only in the Expert Summary displays (and in the Classic display window). For more information on the **Name width** command, see "Name Width Display Option" on page 4–36.
- There are also several function keys which can speed your navigation through the Expert Overview. These keys are described in "Advanced Navigation Techniques" on page 5–77.

Each level of display has Explain messages. However, you must pause capture before pressing F1 **[Explain]** to invoke them. Explain messages are context-sensitive; their contents change according to the information being displayed. To terminate the display of an Explain screen, press ESC. You can display as many explain messages as you want while capture is paused. Simply switch to another display or highlight a different field in the current display and press F1 to invoke the message for that topic.

The Expert Overview Display

When you start capture in Expert mode, the Expert Overview appears (Figure 5–2). The Expert Overview summarizes network activity at each Expert layer. There are separate counters for the number of network objects, symptoms, and diagnoses detected at each Expert layer, allowing you to maintain a constant overview on the health of your network.

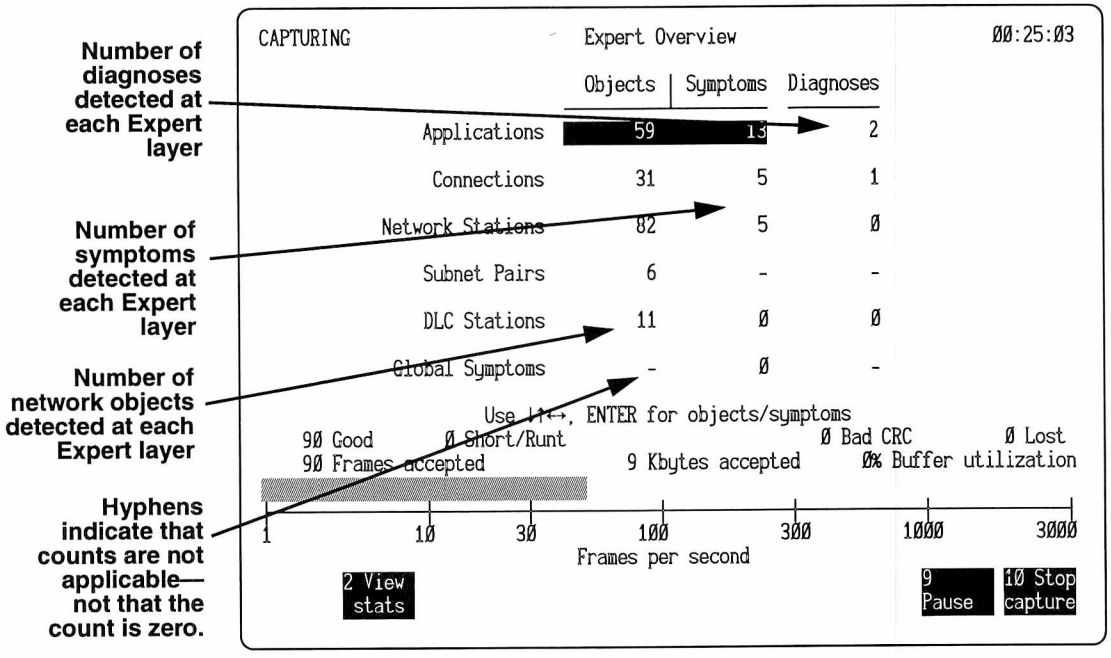


Figure 5–2. The Expert Overview

The Expert Overview is organized as a table with six rows and three columns. The rows represent the four Expert layers, plus one row for subnet pairs and one row for global symptoms. Subnet Pairs and Global Symptoms are not Expert layers. These fields is to provide more information about subnets and global symptoms like traffic bursts.

The three columns include:

- **Objects**—the number of network objects detected at this Expert layer (that is, the number of connections at the Application layer, connections at the Connection layer, Network Stations, and DLC Stations detected since capture started).
- **Symptoms**—the number of symptoms detected at this Expert layer.
- **Diagnoses**—the number of diagnoses detected at this Expert layer.

For definitions of network objects, symptoms, and diagnoses, see "Expert Analyzer Terminology" on page 2–3.

Navigating through the Expert Overview

Each cell within the Expert Overview table is a gateway to more detailed subscreens. By using the cursor keys to highlight a particular field and pressing ENTER, you can see more detailed information about the objects, symptoms, and diagnoses at the highlighted layer. These subdisplays are described in later sections.

While Objects and Symptoms are tabulated separately, you cannot view them separately, because their displays are integrated. The cursor indicates this by highlighting both columns, as in Figure 5–2.

NOTE: The analyzer can only record 100 diagnoses. While it is unlikely that your network will ever reach that many diagnoses, you can limit the number of diagnoses you see. To limit it, set the Expert thresholds higher, or consider setting a capture filter.

Other Counters in the Expert Overview

The Expert Overview shows the same statistics near the bottom of the screen as any capture display. For example, it includes the number of frames captured, the percentage of network usage, buffer utilization, and so on, which you would also see on an analyzer capturing in Classic mode. The exact format depends on the options you select in the **Capture\Screen format** menu. For more information on these counters, see "Information in the Tabular Views" on page 6–17 and "Information in the Skyline View" on page 6–28.

Diagnosis-Related Displays

This section describes the various displays accessible from the **Diagnoses** column of the Expert Overview. For a description of the Expert displays accessible from the **Objects/Symptoms** column of the Expert Overview, see page 5–38.

Diagnosis Summary Window

The Diagnosis Summary window lists all diagnoses generated by the Expert analyzer at the selected Expert layer. The analyzer updates the appropriate diagnosis count in the Expert Overview each time it makes a diagnosis. Each diagnosis is a conclusion that the analyzer makes when predefined thresholds have been exceeded.

NOTE: If the Diagnosis Summary window shows a negative capture time, then the Sniffer Network Analyzer has been capturing for more than 20 days. To correct the negative time, start a new capture session.

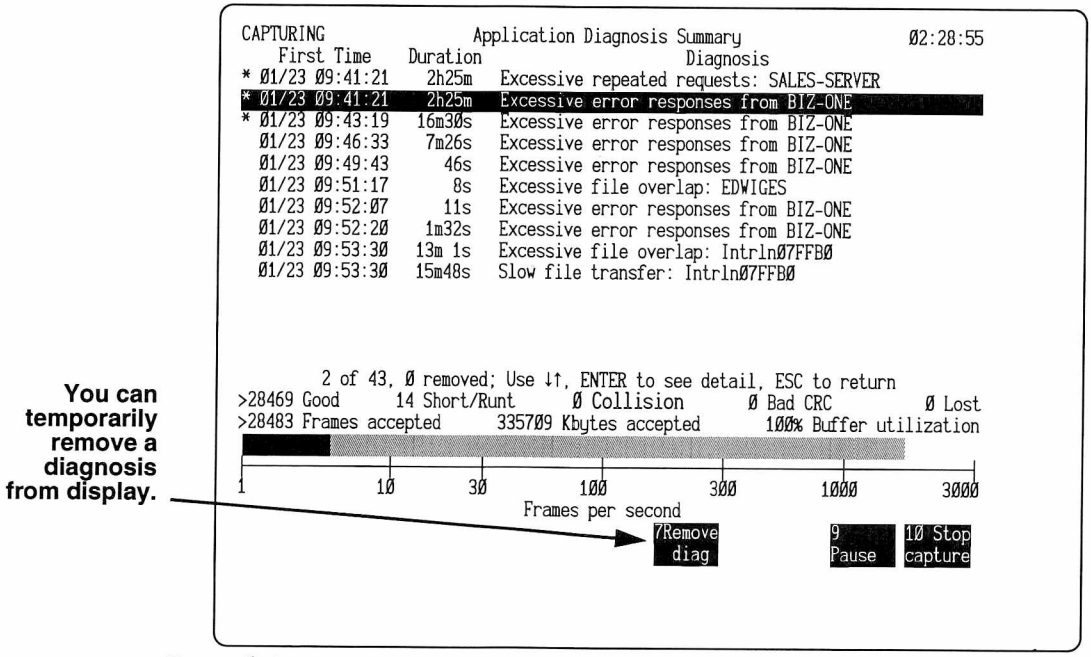
The procedure below explains how to display a Diagnosis Summary window.

To display a Diagnosis Summary window:

1. In the Expert Overview, use the cursor keys to highlight a particular layer in the Diagnoses column that shows at least one diagnosis. Press ENTER.
   Result: The Diagnosis Summary window appears, as shown in Figure 5–3.

NOTE: The Summary window appears only if diagnoses exist at the selected layer.

Each diagnosis in the Summary window represents an important "clue" that might lead to the discovery of a network problem.


CAPTURING
Application Diagnosis Summary
02:28:55
First Time
Duration
Diagnosis
* 01/23 09:41:21 2h25m Excessive repeated requests: SALES-SERVER
* 01/23 09:41:21 2h25m Excessive error responses from BIZ-ONE
* 01/23 09:43:19 16m30s Excessive error responses from BIZ-ONE
01/23 09:46:33 7m26s Excessive error responses from BIZ-ONE
01/23 09:49:43 46s Excessive error responses from BIZ-ONE
01/23 09:51:17 8s Excessive file overlap: EDWIGES
01/23 09:52:07 11s Excessive error responses from BIZ-ONE
01/23 09:52:20 1m32s Excessive error responses from BIZ-ONE
01/23 09:53:30 13m 1s Excessive file overlap: IntrlnØ7FFBØ
01/23 09:53:30 15m48s Slow file transfer: IntrlnØ7FFBØ
2 of 43, Ø removed; Use ↓↑, ENTER to see detail, ESC to return
>28469 Good 14 Short/Runt Ø Collision Ø Bad CRC Ø Lost
>28483 Frames accepted 335709 Kbytes accepted 100% Buffer utilization
1
10
30
100
300
1000
3000
Frames per second
7Remove diag
9 Pause
10 Stop capture

You can temporarily remove a diagnosis from display.

Figure 5–3. Diagnosis Summary window

The following list describes the three types of information shown in the Summary display:

First Time

The time when the analyzer first makes the diagnosis.

Duration

The length of time during which the diagnosis is valid. Suppose the diagnosis is **Excessive error responses from BIZ-ONE**, as in Figure 5–3. This means that the ratio of denied application requests to successful requests has exceeded the **Error resp** threshold in the **Expert config\Thresholds** menu. This condition has been active for a total of two hours and 25 minutes.

An asterisk in the first column indicates that the diagnosis is still active. In the above example, it means that BIZ-ONE is currently denying excessive application requests. The asterisk disappears and the counter for duration stops incrementing when the percentage of denied requests drops below the **Error resp** threshold. If the diagnosis condition begins again, the analyzer will increment the existing counter cumulatively. The duration counter does not imply consecutive time.

Diagnosis	A statement describing a potential network problem. It may or may not be a valid conclusion. Before making a final judgment, you might want to take into account circumstances that are not known to the analyzer.

Press F1 to display the Explain message related to the highlighted diagnosis. The Explain message reminds you of the thresholds that affect the diagnosis and includes suggestions on how to examine other statistics to assess the seriousness of the problem. To return to the Summary display, press ESC.

Temporarily Removing Diagnoses From the Expert Window

During your investigation of network problems, you may want to limit the diagnostic displays in the Expert window to only those problems which currently concern you. The procedure below explains how to temporarily remove a diagnosis from the Expert window.

To remove a diagnosis from the Expert window temporarily:

1. Use the cursor keys to display one of the following:
   - A Diagnosis Summary window
   - A Diagnosis Detail window
2. Highlight the diagnosis which you want to temporarily remove from the display.
3. Notice the dynamic function key label at the bottom of the display for F7 **[Remove diag]**. Figure 5–3 shows the label.

   Press F7 **[Remove diag]** to temporarily remove the highlighted diagnosis from display.

You can remove as many diagnoses as you like, narrowing the display to show only those that concern you. The removed diagnoses have not been erased; they have simply been removed from display. The procedure below explains how to restore them.

To restore removed diagnoses to the display:

1. Use the cursor keys to display one of the following:
   - A Diagnosis Summary window
   - A Diagnosis Detail window
2. If there are diagnoses that have been removed, and can now be restored, the function key label F8 **[Restore diags]** appears. Press F8 to restore the removed diagnoses.

You cannot restore diagnoses individually. Pressing F8 restores all diagnoses removed during the current Expert session.

Diagnosis Detail Displays

Diagnosis Detail displays provide information important to the investigation of a network problem. The exact information in the Detail display depends on the nature of the highlighted diagnosis. For example, the Detail display for the **Slow server** diagnosis lists the addresses of all stations that received a slow response from a given server. This section describes the Detail display for each diagnosis made by the Expert analyzer. The procedure below explains how to view a Diagnosis detail display.

To display a Diagnosis Detail window:

1. In the Expert Overview, use the cursor keys to highlight a particular layer in the Diagnoses column that shows at least one diagnosis. Press ENTER.
2. In the Summary window that appears, use the cursor keys to highlight the diagnosis you want to investigate. Press ENTER.

   The Diagnosis Detail display for the selected diagnosis appears.

Figure 5–4 summarizes the Diagnosis Detail displays and their related Expert thresholds. The displays are organized in alphabetical order.

Diagnosis	Detail Window shown on:	Related Expert Threshold	Threshold described on:
Broadcast Storm	page 5–16	Broadcast Diagnosis	page 4–27
Duplicate Network Address	page 5–17	Duplicate Address Percentage	page 4–24
Excessive Repeated Requests	page 5–18	Filter Time/Loop %	page 4–19
Excessive Requests Denied	page 5–19	Denied Request %	page 4–20
File Overlap/Retransmission	page 5–21	Slow File %	page 4–21
High Rate of Congestion	page 5–22	Receiver Congestion	page 4–28
High Rate of Line/Burst Errors	page 5–23	Ring Errors	page 4–29
High Rate of Physical Errors	page 5–23	Physical Errors	page 4–27
High Rate of Remove from Ring Reqs	page 5–24	Station Removed	page 4–28
High Rate of Ring Entries	page 5–26	Ring Entries	page 4–28
High Rate of Ring Purges	page 5–27	Ring Purge Diagnosis	page 4–29
LAN Overloaded	page 5–28	LAN Overload / LAN Overload % WAN Overload / Overload Timer	page 4–25 page 4–30
Local Router	page 5–29	No threshold	
Multiple Routers to Station	page 5–30	Multiple Routers	page 4–24
Non-responsive Station	page 5–31	No responses	page 4–22
Retransmissions	page 5–33	Retransmission %	page 4–22
Ring beaconing	page 5–34	No threshold	
Slow File Transfer	page 5–35	Slow File %	page 4–21
Slow Server	page 5–36	Response Time/Slow Response %	page 4–18
Underloaded Network	page 5–37	WAN Underload/Underload Timer	page 4–31

Figure 5–4. Diagnosis detail displays and expert thresholds

Broadcast Storm

The analyzer diagnoses a broadcast storm condition when the number of broadcast frames per second exceeds the threshold specified by **Broadcast dg** in the **Expert config** menu. For more information on the **Broadcast dg** threshold, see page 4–27.

The detail display, shown in Figure 5–5, provides the following information:

- **Total number of broadcast storms.** Number of broadcast storm diagnoses made by the analyzer during this capture session. When the number of broadcast frames per second falls below the **Broadcast dg** threshold, the current broadcast storm is considered to be finished. If the threshold is exceeded again, a new broadcast storm diagnosis will be generated.
- **Total number of frames in all storms.** Total number of frames associated with all broadcast storms currently diagnosed by the analyzer.
- **Duration of broadcast storms.** Total length (in seconds) of all broadcast storms currently diagnosed by the analyzer.

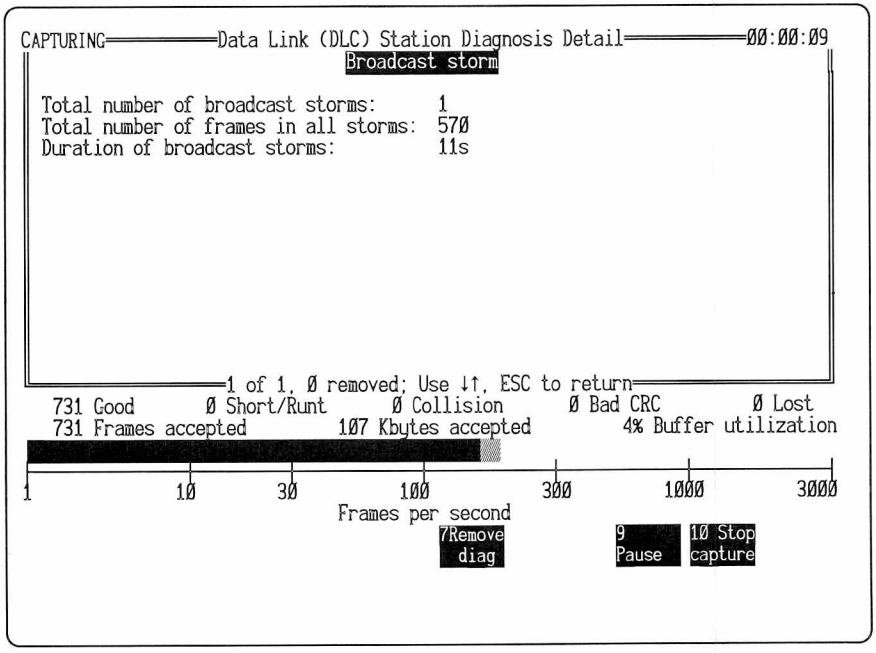


Figure 5–5. Detail display for the diagnosis ***Broadcast storm***

Duplicate Network Address

The analyzer generates the **Duplicate net address** diagnosis when two or more DLC stations are associated with the same network address. In a DECnet environment, the **Duplicate Address percentage** threshold can be used to fine-tune this diagnosis. For more information on the **Duplicate Address percentage** threshold, see page 4–24.

The detail display for the **Duplicate net address** diagnosis provides the following information:

Network address	The network address associated with more than one DLC station.
DLC stations	The addresses of all DLC stations associated with the duplicate network address.

Figure 5–6 shows a typical detail display for the **Duplicate net address** diagnosis. In this example, the network address [192.42.252.50] is associated with both the DLC stations Sun 07972C and IntrIn0591A2.

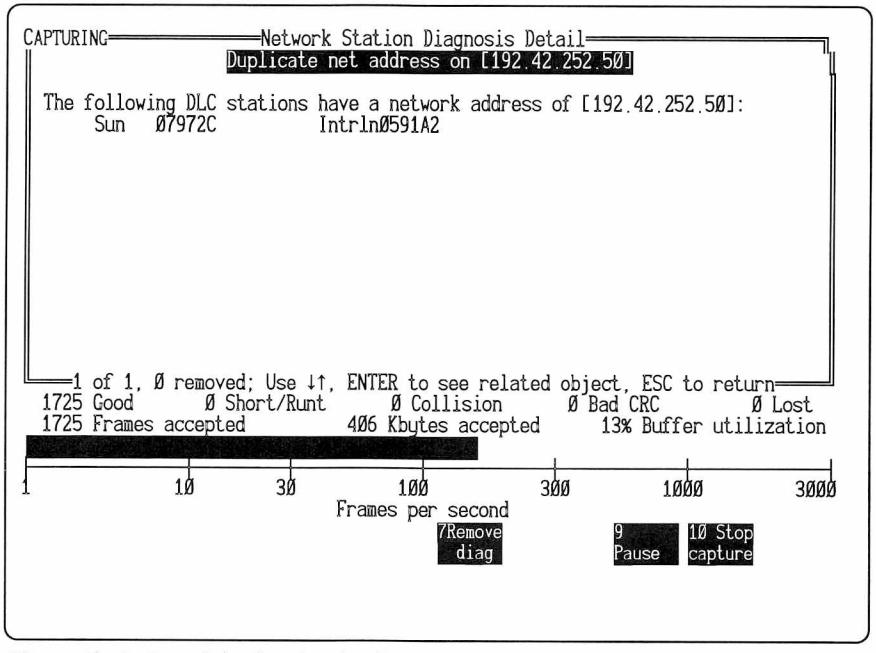


Figure 5–6. Detail display for the diagnosis ***Duplicate net address***

Excessive Repeated Requests

The analyzer generates the **Excessive repeated requests** diagnosis when the number of loops on a given connection exceeds the **Loop** % threshold of total application requests. For more information on the **Loop** % threshold and how the analyzer recognizes loop packets, see the sections "Filter Time," and "Loop Percentage," starting on page 4–19.

The detail display for **Excessive repeated requests** provides the following information:

Total requests loops	The total number of repeated requests sent out by this station. The requests can be of different types.
Mean time between requests	The total amount of time a station sends repeated requests divided by the total number of repeated requests.
Server impacted	Server impacted is the server to which this station sends the repeated requests.

Figure 5–7 shows a typical detail display for the Excessive repeated requests. In this example, the station ANCHOR has sent excessive repeated requests to the server BIZ-ONE.

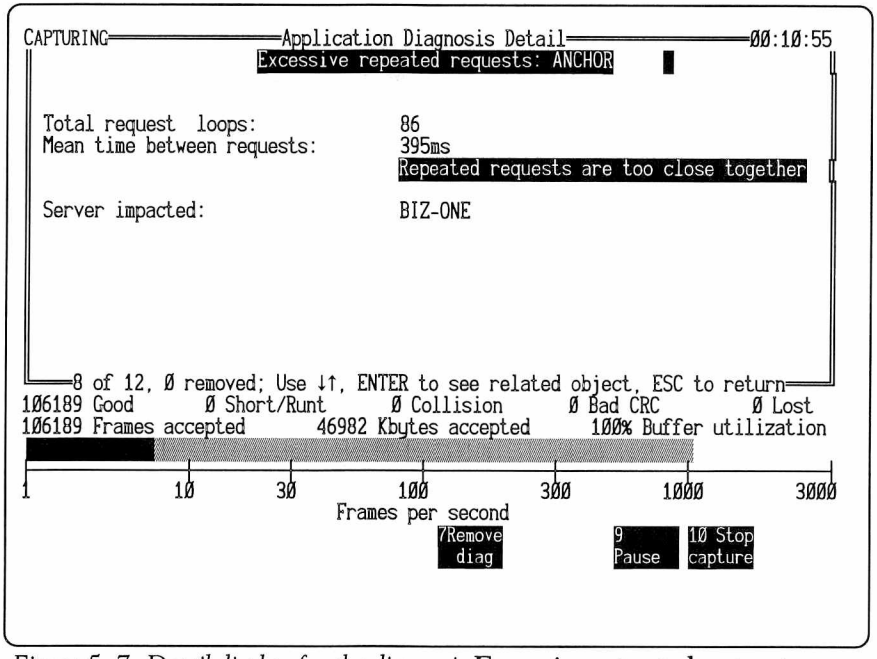

CAPTURING
Application Diagnosis Detail
00:10:55
Excessive repeated requests: ANCHOR
Total request loops: 86
Mean time between requests: 395ms
Repeated requests are too close together
Server impacted: BIZ-ONE
8 of 12, 0 removed; Use ↓↑, ENTER to see related object, ESC to return
106189 Good 0 Short/Runt 0 Collision 0 Bad CRC 0 Lost
106189 Frames accepted 46982 Kbytes accepted 100% Buffer utilization
1 10 30 100 300 1000 3000
Frames per second
7 Remove diag
9 Pause
10 Stop capture

Figure 5–7. Detail display for the diagnosis ***Excessive repeated requests***

Excessive Requests Denied

The analyzer generates the diagnosis **Excessive requests denied** when the percentage of denied versus successful application requests exceeds the **Denied request %** threshold in the **Expert config** menu. For more information on this threshold, see page 4–20.

The information provided by the detail display for this diagnosis is described at the left of Figure 5–8.

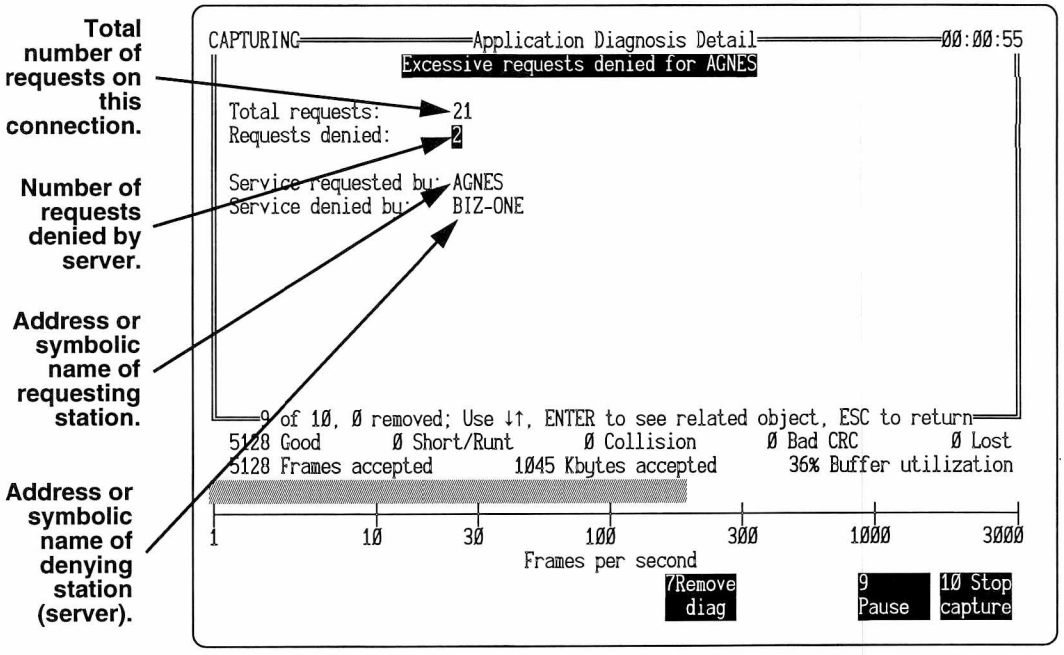


Figure 5–8. Detail display for the diagnosis ***Excessive requests denied***

File Overlap / Retransmission

The analyzer generates the **File overlap/retransmission** diagnosis when the percentage of file transfers that are retransmissions has exceeded the **Slow file%** threshold in the **Expert config** menu. For more information on this threshold, see page 4–21.

This diagnosis indicates excessive retransmissions of the same file request, or overlap between two file requests. The detail display provides the following information.

- The address or symbolic name of the station sending repeated or overlapping file requests
- The total number of file transfers in which this station was involved
- The number of file transfers which were overlapping file requests
- The number of file transfers which were retransmissions

Figure 5–9 shows the detail display for the **File overlap/retransmission** diagnosis.

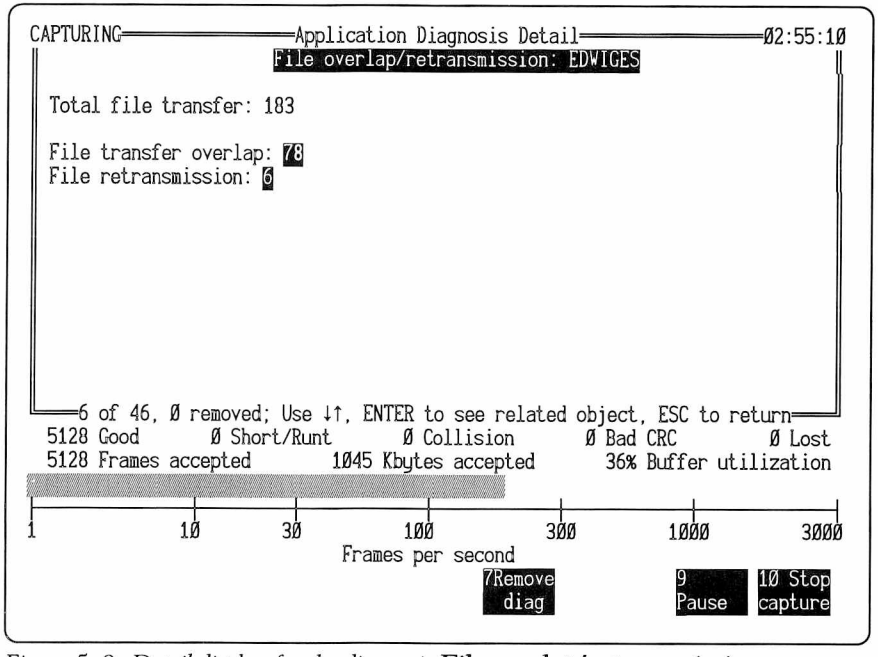


Figure 5–9. Detail display for the diagnosis ***File overlap/retransmission***

High Rate of Congestion

The analyzer generates the **High rate of congestion** diagnosis when it detects a particular station exhibiting more receiver congestion errors per minute than specified by the **RX Congestion** threshold. Receiver congestion errors occur when a station detects a frame on the ring with its own destination address but is unable to copy it because of a lack of buffer space. For more information on the **RX Congestion** threshold, see page 4–28.

Figure 5–10 shows a typical detail display for the **High rate of congestion** diagnosis. In this example, there have been 69 total receiver congestion errors detected for the station MajorDomo. The information provided by this detail display is described at the left of Figure 5–10.

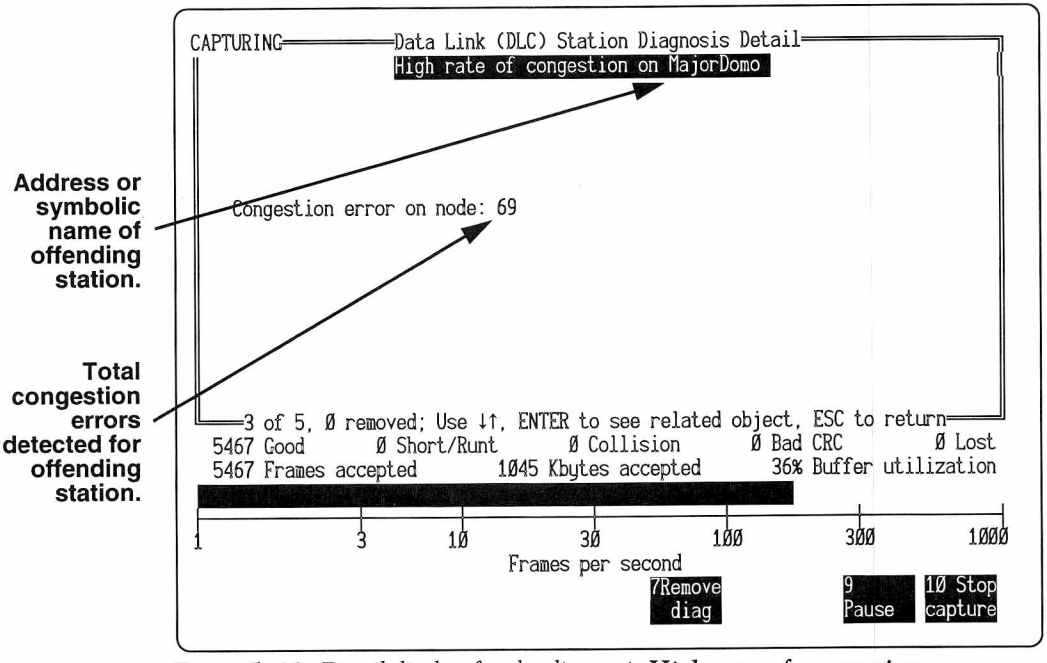


Figure 5–10. Detail display for the diagnosis ***High rate of congestion***

High Rate of Line or Burst Errors

The analyzer generates the **High rate of line/burst errors** diagnosis when the total MAC level line errors plus burst errors for a particular station exceeds the **Ring errors** threshold. For more information on the **Ring errors** threshold, see page 4–29.

Figure 5–11 shows a typical detail display for the **High rate of line/burst errors** diagnosis. In this example, the station AGNES has had a total of 2309 line errors plus burst errors during this capture session. The information provided by this detail display is described at the left of Figure 5–11.

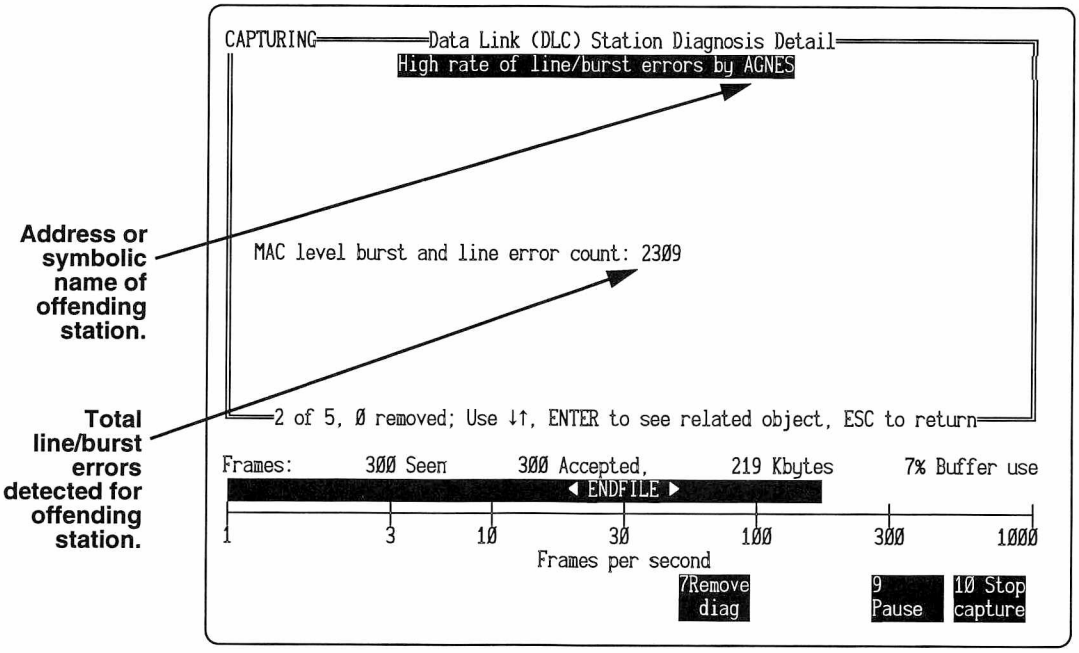

Address or symbolic name of offending station.
Total line/burst errors detected for offending station.
CAPTURING
Data Link (DLC) Station Diagnosis Detail
High rate of line/burst errors by AGNES
MAC level burst and line error count: 2309
2 of 5, Ø removed; Use ↓↑, ENTER to see related object, ESC to return
Frames: 3ØØ Seen 3ØØ Accepted, 219 Kbytes 7% Buffer use
◀ ENDFILE ▶
1 3 1Ø 3Ø 1ØØ 3ØØ 1ØØØ
Frames per second
7Remove diag
9 Pause
1Ø Stop capture

Figure 5–11. Detail display for the diagnosis ***High rate of line/burst errors***

High Rate of Physical Errors

The analyzer generates the diagnosis **High rate of physical errors** when the number of physical errors per second detected for a given station exceeds the **Physical err** threshold in the Expert config menu. For more information on how the analyzer tracks physical errors, refer to page 4–27.

The detail display for the **High rate of physical errors** diagnosis includes the following information:

Name — The address or symbolic name of the offending station.

Packet count	The total number of packets exhibiting physical errors sent by the offending station. Press ENTER to see the Network Object Detail display. It shows the number of physical error packets sent and received by the offending station.
Physical error rate	The maximum rate of physical error packets per second sent by the offending station.

Figure 5–12 shows a typical detail display for the **High rate of physical errors** diagnosis. In this example, the station SALES has transmitted a total of 266 packets exhibiting physical errors. The maximum rate at which these physical error packets were sent was 14 per second, exceeding the default **Physical err** threshold of four per second per station.

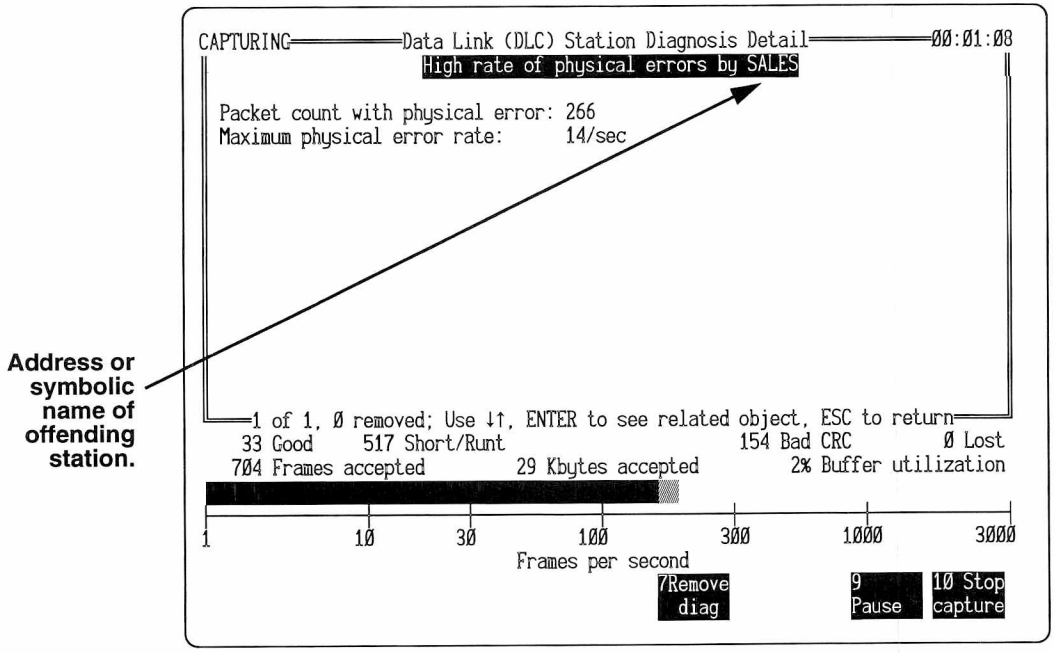

Address or symbolic name of offending station.
CAPTURING
Data Link (DLC) Station Diagnosis Detail
ØØ:Ø1:Ø8
High rate of physical errors by SALES
Packet count with physical error: 266
Maximum physical error rate: 14/sec
1 of 1, Ø removed; Use ↓↑, ENTER to see related object, ESC to return
33 Good 517 Short/Runt 154 Bad CRC Ø Lost
7Ø4 Frames accepted 29 Kbytes accepted 2% Buffer utilization
1 1Ø 3Ø 1ØØ 3ØØ 1ØØØ 3ØØØ
Frames per second
7Remove diag
9 Pause
1Ø Stop capture

Figure 5–12. Detail display for the diagnosis ***High rate of physical errors***

High Rate of Remove from Ring Requests

The analyzer generates the diagnosis **High rate of remove from ring requests** when the rate of Remove from Ring requests detected by the analyzer exceeds the **Station Removed** threshold in the Expert config menu. Remove from Ring requests are sent by the Configuration Report Server, a virtual ring entity responsible for overall ring health. For more information on the **Station Removed** threshold, see page 4–28.

Figure 5–13 shows a typical detail display for the **High rate of remove from ring requests** diagnosis. The display shows the number of remove from ring requests per minute detected by the analyzer. Pressing ENTER from this display shows the addresses of the stations to which remove from ring requests have been sent.

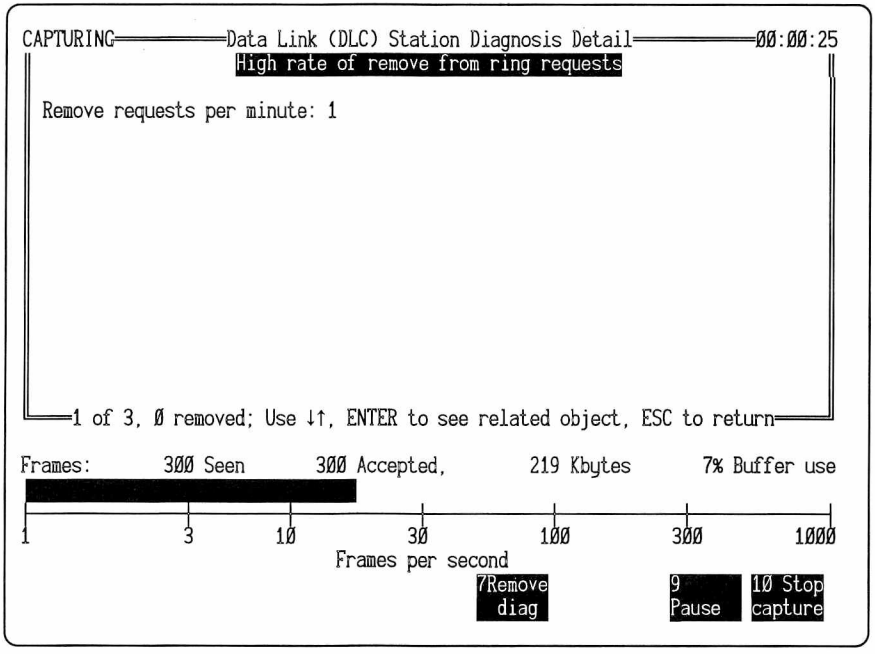


Figure 5–13. Detail display for the diagnosis ***High rate of remove from ring requests***

High Rate of Ring Entries

The analyzer generates the **High rate of ring entry** diagnosis when the number of ring entries per minute for a given station exceeds the **Ring entries** threshold. For more information on the **Ring entries** threshold, see page 4–28.

Figure 5–14 shows a typical detail display for the **High rate of ring entry** diagnosis. In this example, the station AGNES has entered the ring five times. The information provided by this display is described at the left of Figure 5–14.

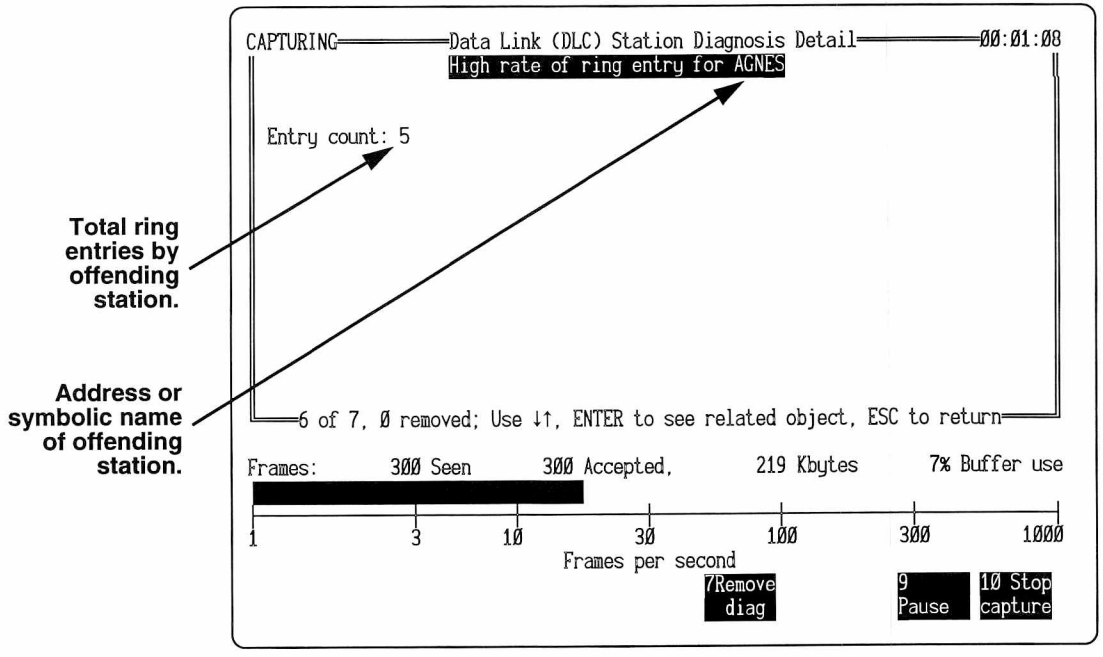


Figure 5–14. Detail display for the diagnosis ***High rate of ring entry***

High Rate of Ring Purges

The analyzer generates the **High rate of ring purges** diagnosis when the number of purge frames per minute sent by a given station exceeds the threshold specified by **Rng purge dg** in the Expert config menu. Ring purge frames are sent by the active monitor when it detects that a token has been lost. For more information on the **Rng purge dg** threshold, see page 4–29.

Figure 5–15 shows a typical detail display for the **High rate of ring purges** diagnosis. In this example, the station SALES-323 has sent a total of 1899 ring purge frames during this capture session. The information in the detail display for this diagnosis is described at the left of Figure 5–15.

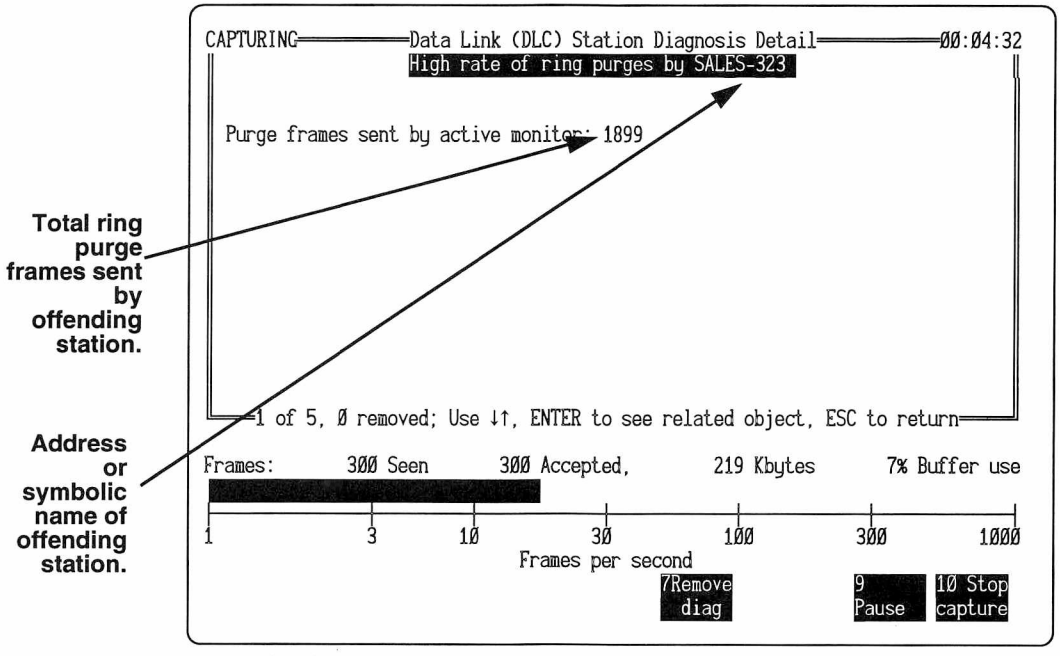

Total ring purge frames sent by offending station.
Address or symbolic name of offending station.
CAPTURING
Data Link (DLC) Station Diagnosis Detail
00:04:32
High rate of ring purges by SALES-323
Purge frames sent by active monitor: 1899
1 of 5, 0 removed; Use ↓↑, ENTER to see related object, ESC to return
Frames: 300 Seen 300 Accepted, 219 Kbytes 7% Buffer use
1 3 10 30 100 300 1000
Frames per second
7Remove diag
9 Pause
10 Stop capture

Figure 5–15. Detail display for the diagnosis ***High rate of ring purges***

LAN Overloaded

The analyzer generates the **LAN overloaded** diagnosis when the percentage of each minute the network is in burst mode exceeds the **LAN overload** % threshold. Whether the network is considered to be in burst mode depends on the setting of the **LAN overload** threshold. For a detailed discussion of these two thresholds and how they interact, see page 4–25.

Because the **LAN overloaded** diagnosis is directly related to the quantity of **Network overload** symptoms, the detail display shows the name or symbolic address of each network station whose traffic is associated with a **Network overload** symptom. Included in the display is the exact number of **Network overload** symptoms with which each particular station is associated. The stations are organized in descending order. Figure 5–16 shows the detail display for the **LAN overloaded** diagnosis.

Each listed station is associated with one or more Network overload symptoms. The number in parentheses shows exactly how many. Notice that the stations are organized in descending order.

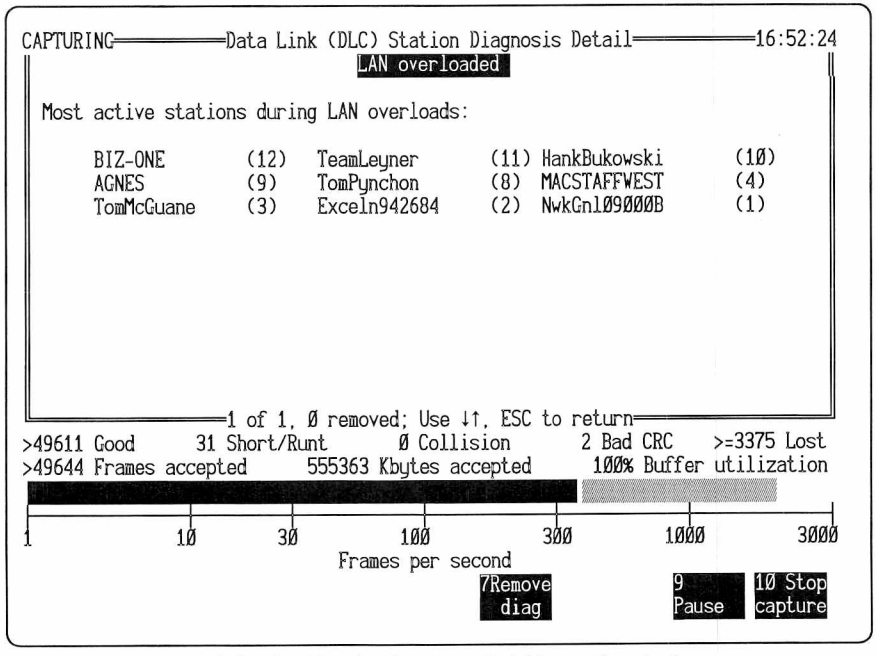

CAPTURING Data Link (DLC) Station Diagnosis Detail 16:52:24
LAN overloaded
Most active stations during LAN overloads:
BIZ-ONE (12) TeamLeyner (11) HankBukowski (10)
AGNES (9) TomPynchon (8) MACSTAFFWEST (4)
TomMcGuane (3) Excel n942684 (2) NwkGnl090000B (1)
1 of 1, 0 removed; Use ↓↑, ESC to return
>49611 Good 31 Short/Runt 0 Collision 2 Bad CRC >=3375 Lost
>49644 Frames accepted 555363 Kbytes accepted 100% Buffer utilization
1 10 30 100 300 1000 3000
Frames per second
7Remove diag
9 Pause
10 Stop capture

Figure 5–16. Detail display for the diagnosis ***LAN overloaded***

Local Router

The analyzer generates the diagnosis **Local router** when two DLC stations on the same network segment are communicating via one or more routers, rather than directly from one DLC station to the other.

The detail display for this diagnosis is shown in Figure 5–17. The information in the detail display is described at the left of Figure 5–17.

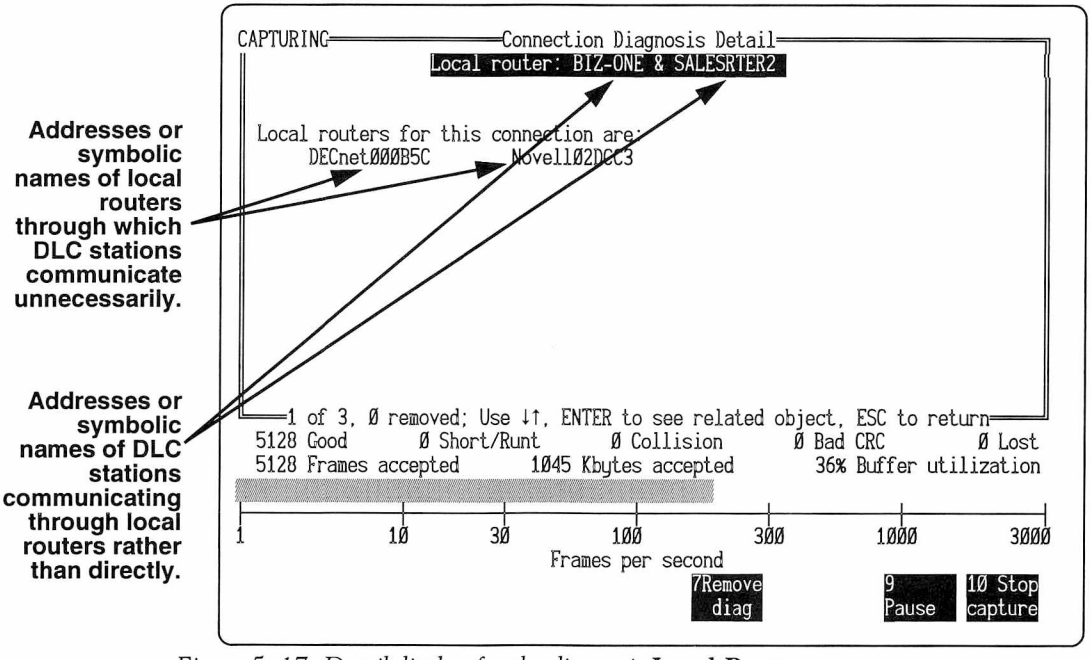


Figure 5–17. Detail display for the diagnosis ***Local Router***

Multiple Routers to Station

The analyzer generates the diagnosis **Multiple routers to station *address*** when there are more routers on the local network that can route to a remote station than specified by the **Multiple routers** threshold in the **Expert config** menu. For more information on the **Multiple routers** threshold, see page 4–24.

The detail display for the diagnosis **Multiple routers to station** is shown in Figure 5–18. The information in the detail display is described at the left of Figure 5–18.

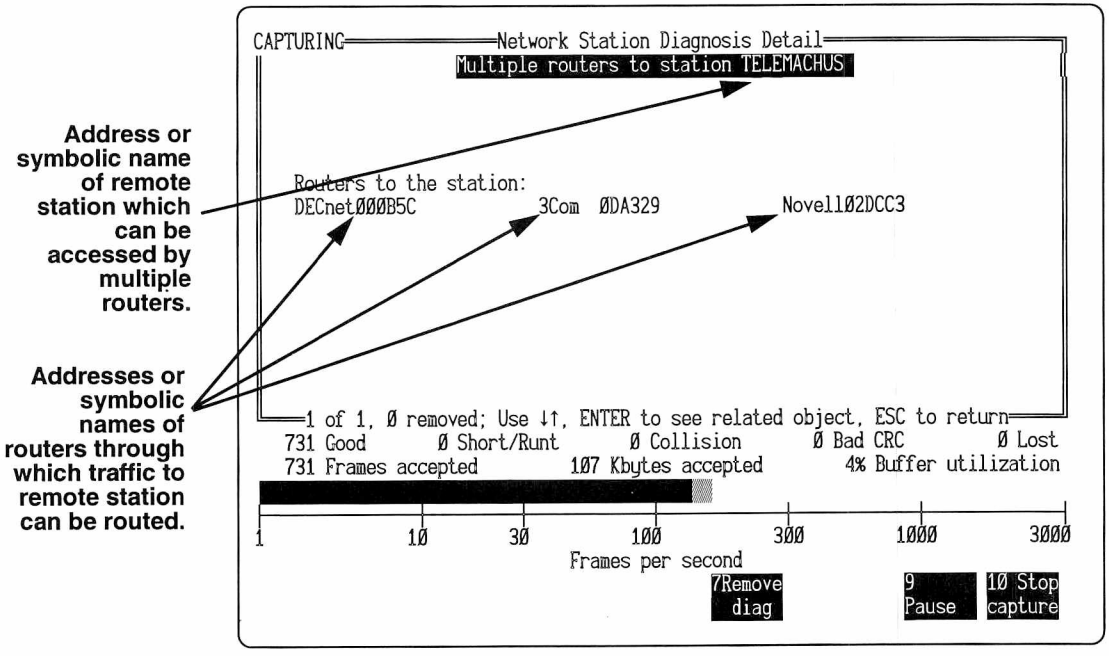


Figure 5–18. Detail display for the diagnosis ***Multiple routers to station***

Non-Responsive Station

The analyzer generates the diagnosis **Non-responsive station** (and considers a connection broken) when the number of consecutive identical retransmissions without response on a given connection exceeds the **No Responses** threshold in the **Expert config** menu.

The analyzer considers a broken connection to start when the number of retransmissions exceeds the **No responses** threshold and to end when the sender sends a new packet. Figure 5–19 illustrates how the analyzer calculates the duration of a broken connection.

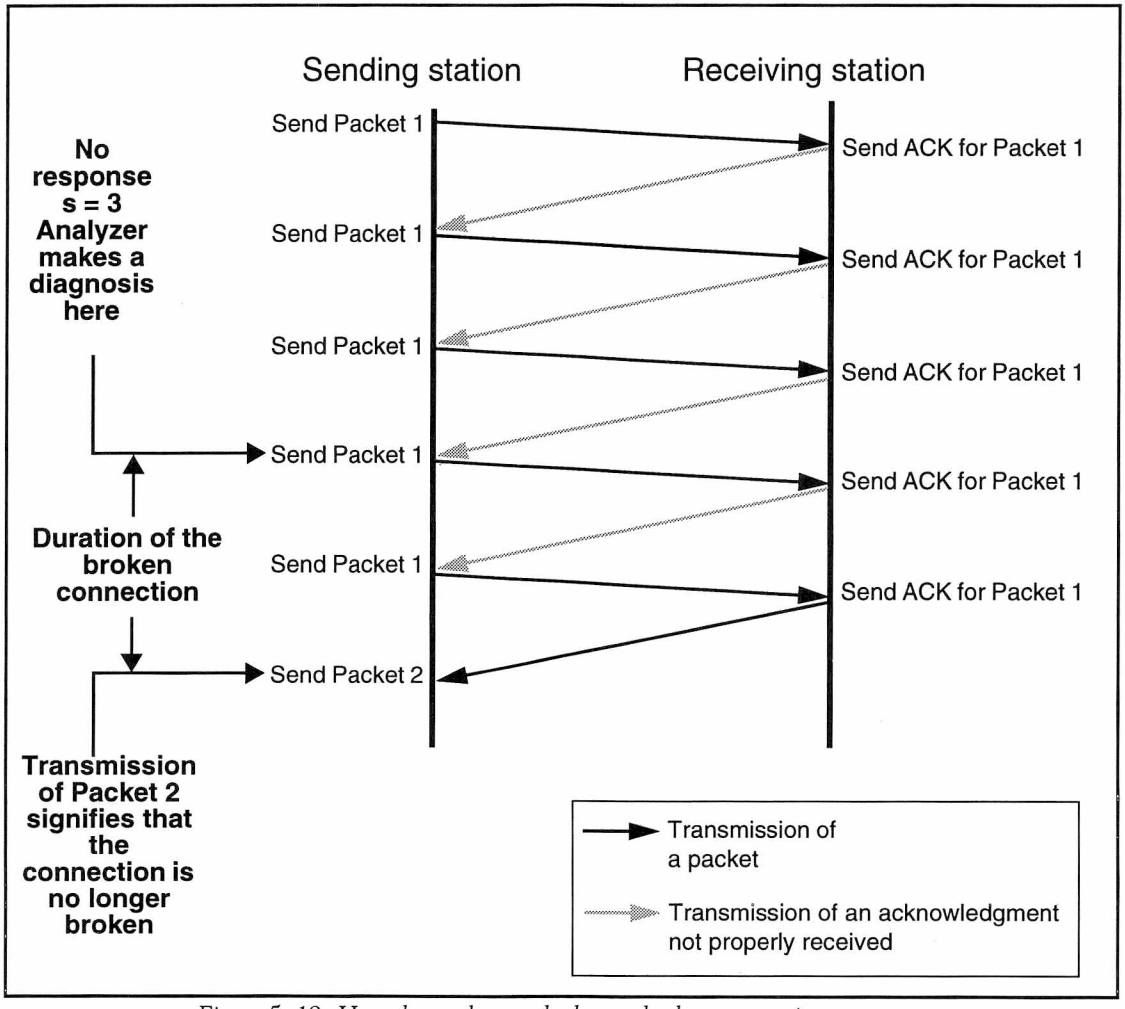

Sending station
Receiving station
Send Packet 1
Send ACK for Packet 1
Send Packet 1
Send ACK for Packet 1
Send Packet 1
Send ACK for Packet 1
Send Packet 1
Send ACK for Packet 1
Send Packet 1
Send ACK for Packet 1
Send Packet 2
No response s = 3 Analyzer makes a diagnosis here
Duration of the broken connection
Transmission of Packet 2 signifies that the connection is no longer broken
Transmission of a packet
Transmission of an acknowledgment not properly received

Figure 5–19. How the analyzer calculates a broken connection

Figure 5–20 shows the detail display for the diagnosis **Non-responsive station.** For more information on the **No responses** threshold, see page 4–22.

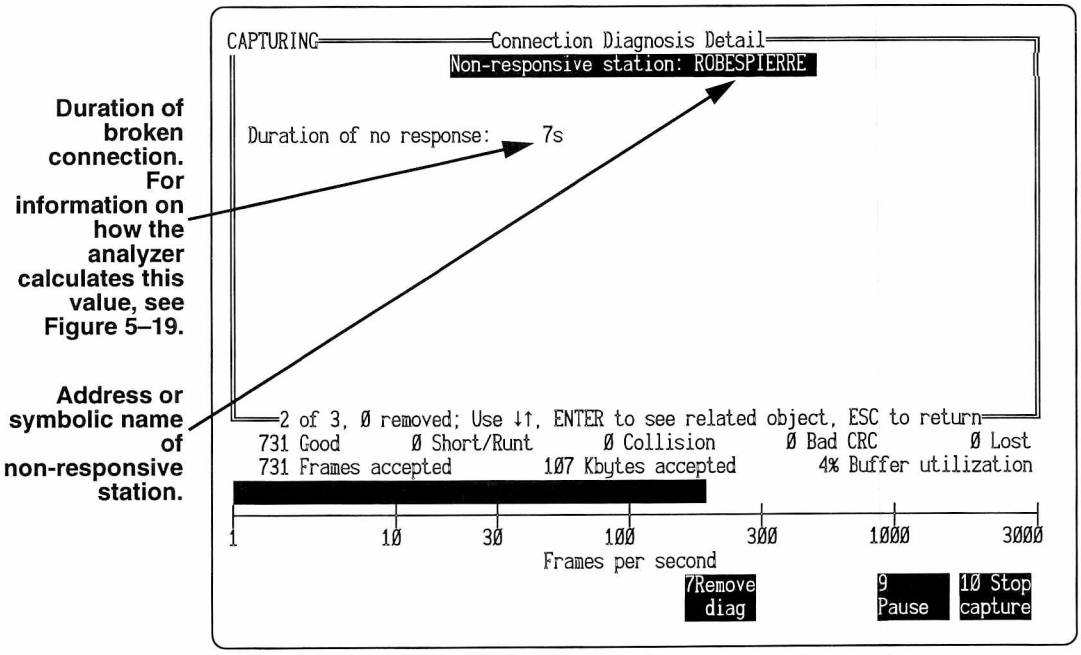


Figure 5–20. Detail display for the diagnosis ***Non-responsive station***

Retransmissions

The analyzer generates the **Retransmissions** diagnosis when the number of retransmissions (expressed as a percentage of total frames on the connection) exceeds the **Retrans** % threshold. For more information on the **Retrans** % threshold, see page 4–22.

The detail display for the **Retransmissions** diagnosis provides the following information:

- The addresses or symbolic names of the endpoint of the connection exhibiting the **Retransmission** diagnosis
- The total number of frames sent on this connection
- The number of frames retransmitted on this connection

Figure 5–21 shows a typical detail display for the **Retransmissions** diagnosis. In this example, 29 frames have passed between the server RND and the workstation AGNES. Of these 29 frames, two were retransmissions.

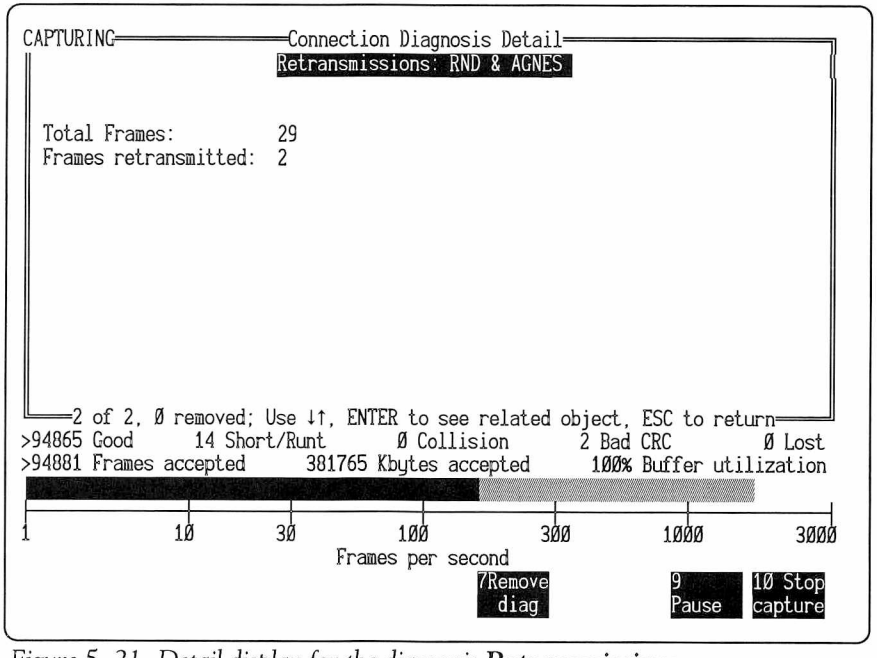

CAPTURING
Connection Diagnosis Detail
Retransmissions: RND & AGNES
Total Frames: 29
Frames retransmitted: 2
2 of 2, Ø removed; Use ↓↑, ENTER to see related object, ESC to return
>94865 Good 14 Short/Runt Ø Collision 2 Bad CRC Ø Lost
>94881 Frames accepted 381765 Kbytes accepted 100% Buffer utilization
1 10 30 100 300 1000 3000
Frames per second
7Remove diag
9 Pause
10 Stop capture

Figure 5–21. Detail display for the diagnosis ***Retransmissions***

Ring Beaconing

The analyzer generates the **Ring beaconing** diagnosis when it detects a single MAC beacon frame. Beacon frames indicate that there is a problem in the token ring that makes the ring inoperable. A ring can be beaconing due to a physical break in the ring or a timeout during active monitor contention.

The information at the left of Figure 5–22 describes the contents of a typical detail display for the **Ring beaconing** diagnosis.

Number of MAC level beacon frames detected by the analyzer.

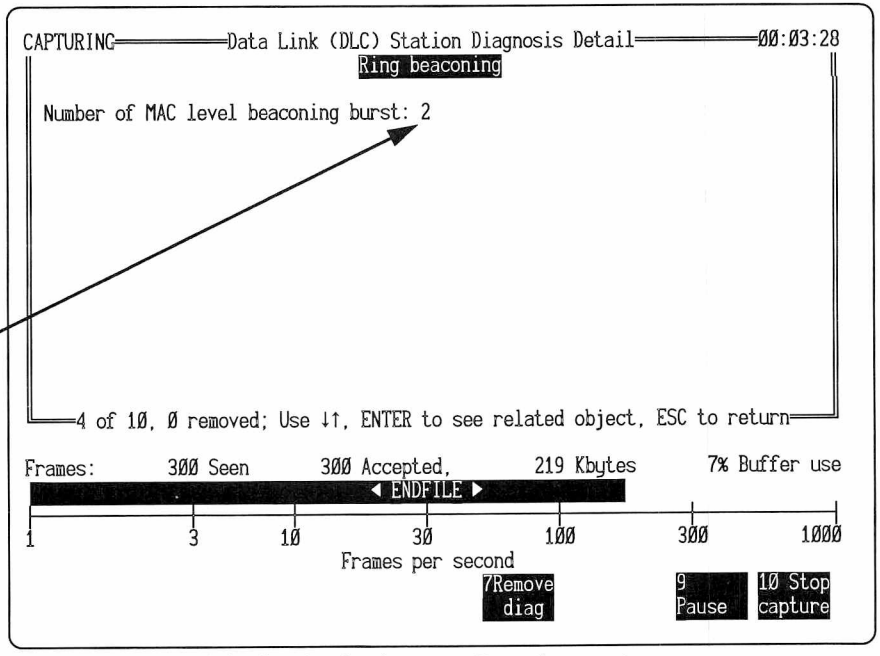

CAPTURING
Data Link (DLC) Station Diagnosis Detail
00:03:28
Ring beaconing
Number of MAC level beaconing burst: 2
4 of 10, 0 removed; Use ↓↑, ENTER to see related object, ESC to return
Frames: 300 Seen 300 Accepted, 219 Kbytes 7% Buffer use
◀ ENDFILE ▶
1 3 10 30 100 300 1000
Frames per second
7Remove diag
9 Pause
10 Stop capture

Figure 5–22. Detail display for the diagnosis ***Ring beaconing***

Slow File Transfer

The analyzer generates the **Slow file transfer** diagnosis when the ratio of slow versus normal file transfers is greater than the **Slow file** % threshold in the Expert config menu. For more information on this threshold and how the analyzer determines whether a file transfer is "slow," see the Denied Request Percentage and Slow File Percentage sections, starting on page 4–20.

The detail display for the **Slow file transfer** diagnosis shows the address or symbolic name of the station that requests the file transfer, as well as the number of slow file transfers versus total file transfers. Figure 5–23 shows a typical detail screen for the **Slow file transfer** diagnosis.

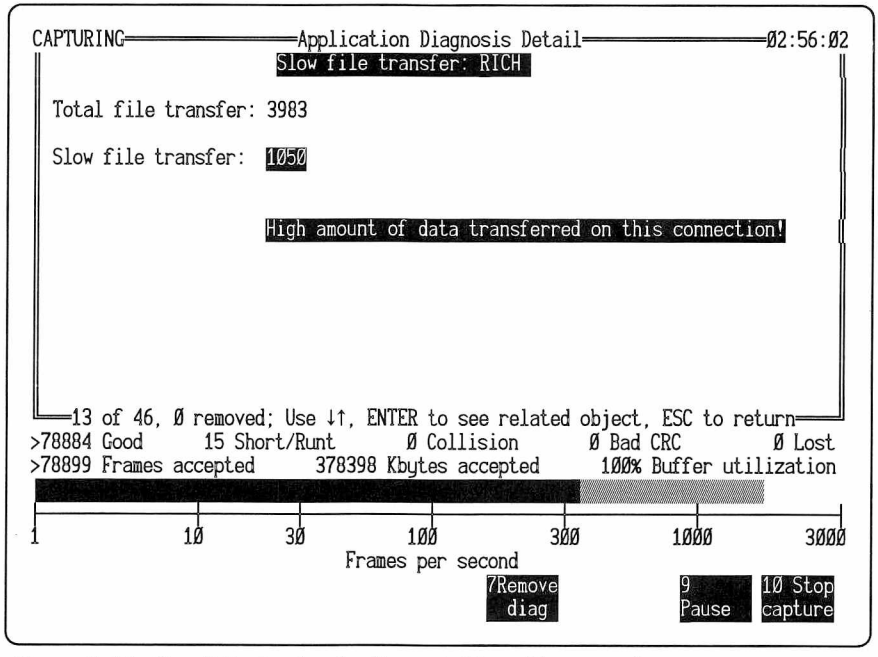


Figure 5–23. Detail display for the diagnosis ***Slow file transfer***

In Figure 5–23, the analyzer has printed the message, "`High amount of data transferred on this connection!`" When the Expert analyzer notices a network event it considers particularly troublesome, it will sometimes print a warning message directly on the screen. In this case, the workstation, "RICH," is involved in a dangerously high-traffic connection. To view statistics on this connection, press ENTER to see the Application Detail screen containing the address of the server responding to Rich's requests and any symptoms that may be associated with this connection.

Slow Server

The analyzer generates the **Slow server** diagnosis when the ratio of slow responses to total responses for a particular station exceeds the **Slow resp** % threshold in the Expert config menu. For more information on this threshold and how the analyzer determines whether a response is "slow," see the "Minimum Application Requests" and "Response Time" sections, starting on page 4–18.

The detail display for the **Slow server** diagnosis shows the address or symbolic name of the slow server. The display also shows the address or symbolic name of each station that has received a slow response from the named server. The analyzer adds a station name to the list as soon as it detects that the station has received a slow response from this server. Figure 5–24 shows the detail display for the **Slow server** diagnosis.

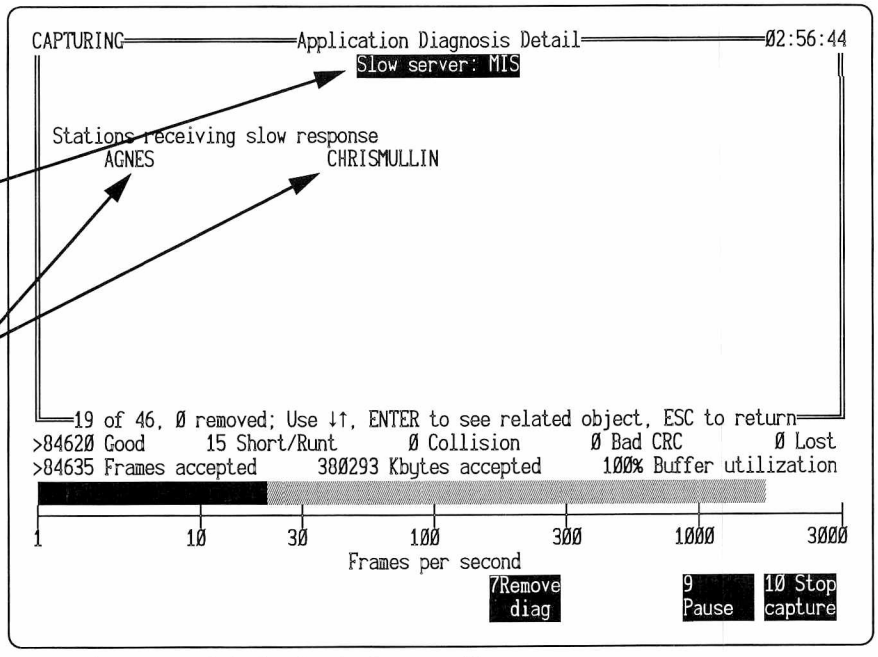


Figure 5–24. Detail display for the diagnosis ***Slow server***

Underloaded Network

The analyzer generates the **Underloaded network** diagnosis when the duration of an underload condition exceeds the **Underload Timer** threshold. Whether the network is considered to be in an underload condition depends on the setting of the **WAN underload** threshold. If the network load (for both DTE and DCE) is less than that specified by **WAN underload**, then the analyzer considers the network to be in an underload condition. For a detailed discussion of these two thresholds and how they interact, see page 4–31.

The detail display shows the name or symbolic address of the most active stations during the WAN underload.

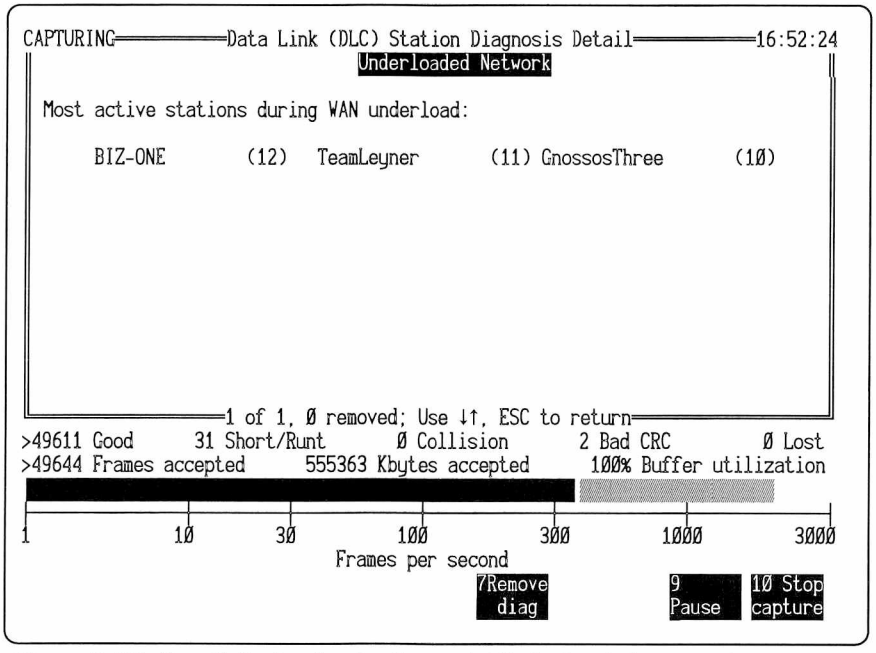

CAPTURING
Data Link (DLC) Station Diagnosis Detail
16:52:24
Underloaded Network
Most active stations during WAN underload:
BIZ-ONE (12) TeamLeyner (11) GnossosThree (1Ø)
1 of 1, Ø removed; Use ↓↑, ESC to return
>49611 Good 31 Short/Runt Ø Collision 2 Bad CRC Ø Lost
>49644 Frames accepted 555363 Kbytes accepted 1ØØ% Buffer utilization
1 1Ø 3Ø 1ØØ 3ØØ 1ØØØ 3ØØØ
Frames per second
7Remove diag
9 Pause
1Ø Stop capture

Figure 5–25. Detail display for the diagnosis ***Underloaded network***

Symptom and Network Object-Related Displays

This section describes the various displays accessible from the **Objects/Symptoms** column of the Expert Overview. The Expert displays accessible from the **Diagnoses** column of the Expert Overview are described starting on page 5–10. Note that the same displays are available in the Expert window regardless of whether the analyzer is capturing or displaying frames.

About Symptom and Network Object-Related Displays

Symptom and Network Object displays are similar to the various diagnosis-related displays, except that:

- The counts pertain to symptoms detected, not diagnoses.
- Even if no symptoms are detected at a particular layer, you can still select that layer and press ENTER to display a list of connections, network addresses, or DLC addresses.
- The **Objects/Symptoms** column also displays pairs of communicating subnets. You can highlight the subnet field and press ENTER to see a list of communicating subnet pairs. (This field provides more information about the subnets; symptoms are not associated with subnets.)
- The **Objects/Symptoms** column also displays Global Symptoms. Global symptoms include LAN and WAN Overloads.

You can navigate through the symptom and network object-related displays just as you would the diagnosis-related displays. Highlighting a field and pressing ENTER causes a Summary window to appear. However, the Symptom and Network Object Summary displays are different from the Diagnosis Summary displays; they display a list of ***all*** network objects detected by the Expert analyzer instead of just those exhibiting symptoms.

Symptom and Network Object Summary Windows

Symptom and Network Object Summary windows provide a list of all network objects detected by the Expert analyzer at the highlighted Expert layer. The Summary windows act as a gateway to the more detailed windows, summarizing general data about the various applications, connections, network stations, and DLC stations detected by the analyzer.

For example, Figure 5–26 shows the Summary window at the Expert Application layer. It lists all the Application layer connections detected by the analyzer during this capture session, the addresses of the connecting stations, the number of frames that have passed between the two stations, and the number of symptoms associated with

those frames. From here, the display shows that the connection between the workstation, BLAIR, and the server BIZ-ONE currently has 123 associated symptoms, including the last symptom detected, **Low throughput**. You can explore this connection further by highlighting it and pressing ENTER to see the related Detail window.

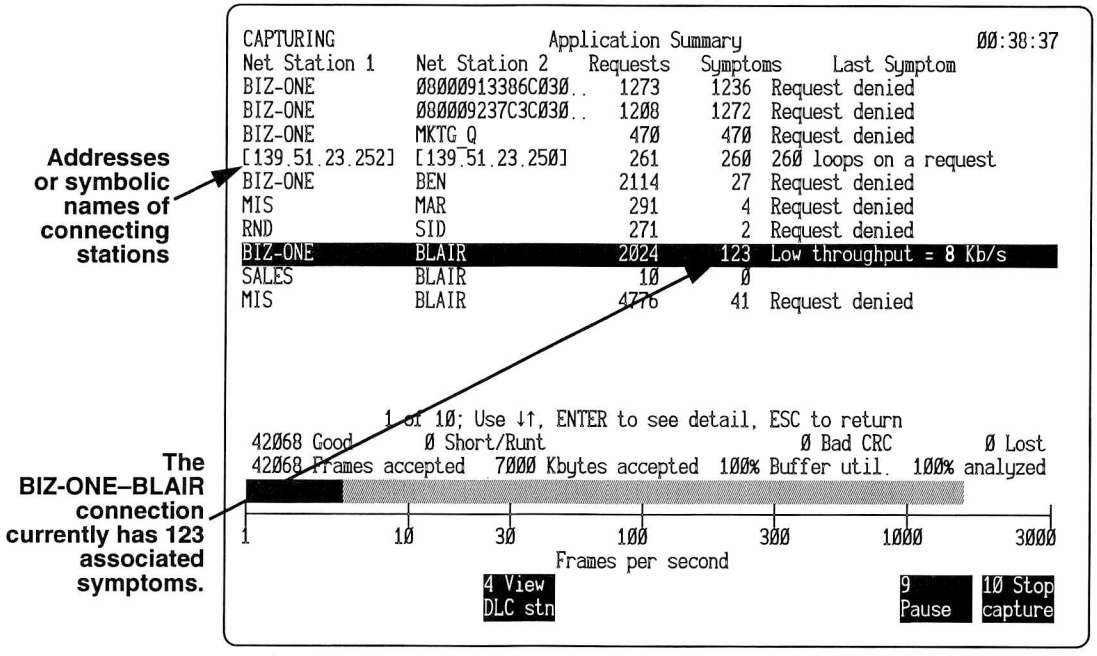

Addresses or symbolic names of connecting stations
The BIZ-ONE–BLAIR connection currently has 123 associated symptoms.
CAPTURING
Application Summary
ØØ:38:37
Net Station 1
Net Station 2
Requests
Symptoms
Last Symptom
BIZ-ONE ØØØØØ913386CØ3Ø.. 1273 1236 Request denied
BIZ-ONE ØØØØØ9237C3CØ3Ø.. 12ØØ 1272 Request denied
BIZ-ONE MKTG_Q 47Ø 47Ø Request denied
[139.51.23.252] [139.51.23.25Ø] 261 26Ø 26Ø loops on a request
BIZ-ONE BEN 2114 27 Request denied
MIS MAR 291 4 Request denied
RND SID 271 2 Request denied
BIZ-ONE BLAIR 2Ø24 123 Low throughput = 8 Kb/s
SALES BLAIR 1Ø Ø
MIS BLAIR 4776 41 Request denied
1 of 1Ø; Use ↓↑, ENTER to see detail, ESC to return
42Ø68 Good Ø Short/Runt Ø Bad CRC Ø Lost
42Ø68 Frames accepted 7ØØØ Kbytes accepted 1ØØ% Buffer util. 1ØØ% analyzed
1 1Ø 3Ø 1ØØ 3ØØ 1ØØØ 3ØØØ
Frames per second
4 View DLC stn
9 Pause
1Ø Stop capture

Figure 5–26. Symptom and Network Object Summary window at the Expert Application layer

Displaying the Summary Window

The following procedure describes how to display the Summary window at any of the Expert layers.

To display a Summary window at any of the Expert layers:

1. From the Symptom and Network Object Overview, use the cursor keys to highlight the desired Expert layer. The Expert layers include:
   - Application Layer
   - Connection Layer
   - Network Station Layer
   - Subnet Pairs

- DLC Station Layer
- Global Symptoms

Subnet Pairs and **Global Symptoms** are not true Expert layers. These fields provide more information about communicating subnet pairs and global symptoms like traffic bursts.

2. Press ENTER.

   Result: The Summary window for the selected layer appears, displaying a list of connections, network addresses, or DLC addresses. The exact format of the display depends on the Expert layer selected.

Information in the Summary Windows

The information presented in the Summary windows is very similar at each of the four Expert layers. However, the Subnet Pairs and Global Symptom windows are slightly different. Those windows are described in later sections.

The Summary windows for the Network Station and DLC layers contains less information than those at the Application and Connection layers. This is because the analyzer detects information for single stations at the Network Station and DLC layers, whereas at the Application and Connection layers it detects information about connections between two stations. This means that there is twice as much address information to present in the Summary windows for these Expert layers.

Figure 5–27 is an example of the Summary window at the Network Station layer. The information presented is very similar to that in Figure 5–26 but for only one station.

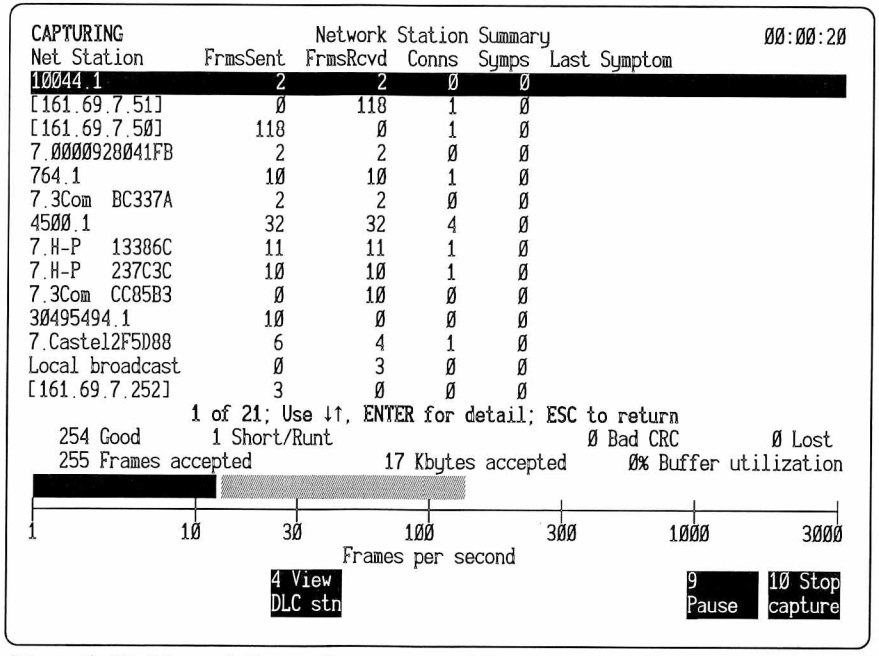

CAPTURING
Network Station Summary
00:00:20
Net Station FrmsSent FrmsRcvd Conns Symps Last Symptom
10044.1 2 2 0 0
[161.69.7.51] 0 118 1 0
[161.69.7.50] 118 0 1 0
7.0000928041FB 2 2 0 0
764.1 10 10 1 0
7.3Com BC337A 2 2 0 0
4500.1 32 32 4 0
7.H-P 13386C 11 11 1 0
7.H-P 237C3C 10 10 1 0
7.3Com CC85B3 0 10 0 0
30495494.1 10 0 0 0
7.Castel2F5D88 6 4 1 0
Local broadcast 0 3 0 0
[161.69.7.252] 3 0 0 0
1 of 21; Use ↓↑, ENTER for detail; ESC to return
254 Good 1 Short/Runt 0 Bad CRC 0 Lost
255 Frames accepted 17 Kbytes accepted 0% Buffer utilization
1 10 30 100 300 1000 3000
Frames per second
4 View DLC stn
9 Pause
10 Stop capture

Figure 5–27. Network Station Summary window

Information Fields in the Summary Windows

The list below summarizes (in alphabetical order) the information fields found in the Summary windows. Not all the information described here is found in every screen. The exact information in the Summary window depends on the Expert layer and the object highlighted.

Bytes — Can be either "Sent bytes," or "Received bytes." Specifies the number of bytes sent or received by the corresponding station. Available only in Network Station or DLC Station Summary window.

Conn — The total number of connections made by this station.

DLC Station Address The DLC addresses of the server, router, or other devices involved in the connection. When the DLC address is not the same as the network address, the analyzer will display the address in parentheses. This can happen when frames are routed to a station from a remote segment. In that case, the analyzer displays the DLC address and name of the router rather than that of the remote station (the net station address will be the actual address of the remote station). See Figure 5–40 on page 5–56 for a graphic representation of this phenomenon.

The analyzer will also display a + sign in front of those DLC stations which have been reached by more than one router.

Frames In the Connection Summary window, **Frames** is the total number of frames transmitted on the specified connection. In the Network Station and DLC Station Summary windows, **Frames** is measured separately for frames sent and frames received by each station detected by the Expert analyzer.

Last Symptom A one-line identifier of the last symptom associated with this connection or station.

Net Station Address The network addresses of the stations involved in the connection. If the Expert analyzer has learned the names associated with the addresses, it will display them instead of the hex, IP, or DECnet addresses.

The analyzer automatically attempts to interpret the first three bytes of the address as the name of the NIC's manufacturer. When it is able to find the manufacturer's code in its table of manufacturers, the analyzer replaces the first three bytes of the station address with an ASCII abbreviation of the manufacturer's name. For example, in Figure 5–28, the characters, "NwkGnl," are substituted for the hex characters 000065.

Protocol A one-line identifier of the protocol used on a connection or by a station. If the analyzer does not recognize the protocol in use, it will substitute the well-known port name (which is usually also a protocol name, such as Telnet or FTP).

Requests The number of application requests made on the highlighted connection.

Symptoms	The total number of symptoms associated with this connection or station.

Keep in mind that the Expert analyzer will dynamically update the Summary window as it learns more about the network to which it is attached. For example, as soon as the analyzer knows the symbolic name associated with a station address, it will substitute that name for the hex address.

Changing the Format of the Summary Window

The information found in each Summary window is a subset of the information in the list above. However, you can vary the information fields in the Summary window at all four Expert layers:

- Application
- Connection
- Network Station
- DLC Station

The following procedure explains how to change the format of the Summary window.

To change the format of the Summary window:

1. Display the Summary window for the desired layer. See page 5–39 for complete instructions.

   Result: Depending on the layer of the Summary window, a label for the function key F4 appears at the bottom of the display. The label for the function key will change depending on the display format it will bring up next. For example, in one view it reads **[View DLC Stn]** and in another **[View protocl]**.

2. Press F4.

   Result: Pressing F4 allows you to cycle through the Summary display formats available at the specified layer. Each time you press F4, the information fields in the Summary window will change.

The following sections describe the various display formats available in the Summary window for each Expert layer.

Application and Connection Layer Summary Window

Figure 5–28 shows the default format for the Application Summary window.

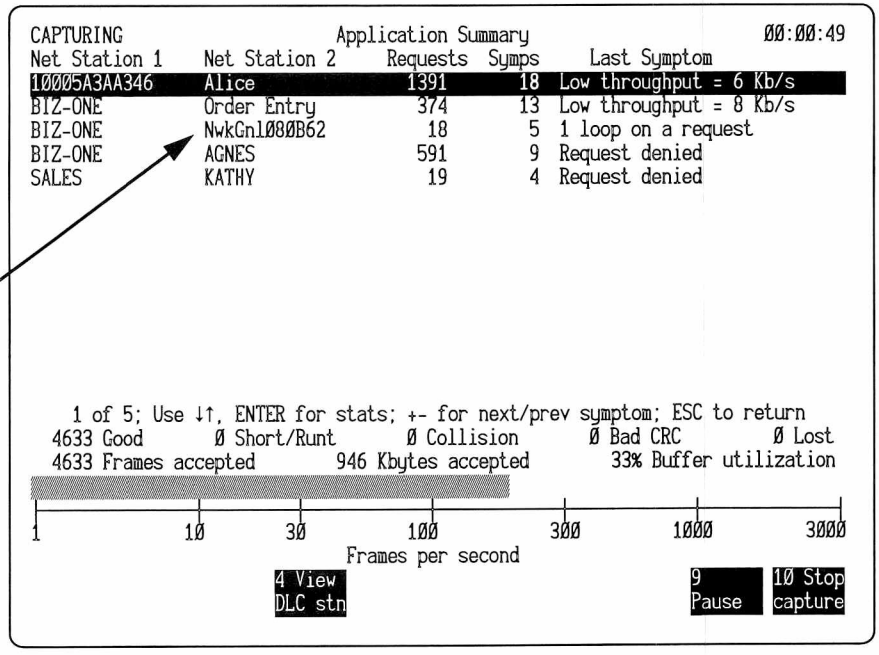


Figure 5–28. The default Application Summary window

The Summary window lists the network addresses of the endpoints of each application layer connection detected by the analyzer. You can also view the connections in terms of the DLC addresses of the two endpoints. The display formats available for the Connection Summary window are exactly the same as those available at the Application layer. The only difference is that the Application Summary window counts application requests while the Connection Summary window counts the total number of frames transmitted on a connection. The available display formats for the Summary windows at the Application and Connection layers are summarized in Figure 5–29.

Shown in...	Format	Column Entries				
Figure 5–28	Net Station Format (default)	Net Station 1	Net Station 2	Requests Frames*	Symptoms	Last Symptom
Figure 5–30	DLC Station Format	DLC Station 1	DLC Station 2	Requests Frames*	Symptoms	Last Symptom
Figure 5–31	Protocol Format	Net Station 1	Net Station 2	Requests Frames*	Symptoms	Protocol

*The Frames counter appears in the Connection Summary window, while the Requests counter appears in the Application Summary window.

Figure 5–29. Application and Connection layer Summary window formats

Figure 5–30 shows the Application Summary window in the DLC Station format.

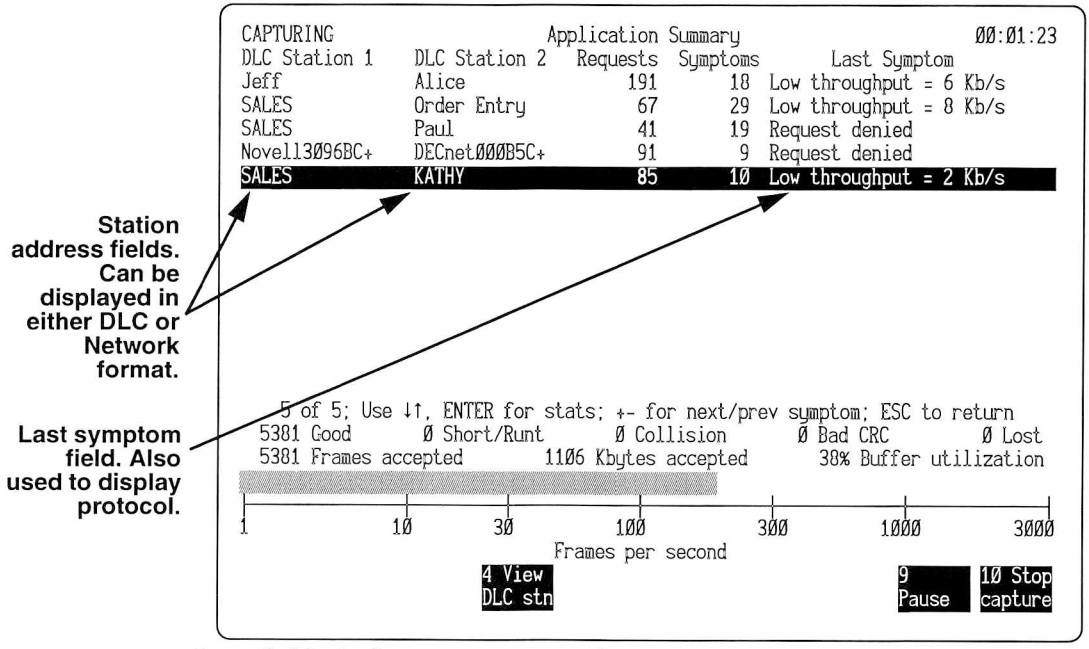


Figure 5–30. Application Summary window in DLC station format

Figure 5–31 shows the Connection Summary window in the Protocol format.

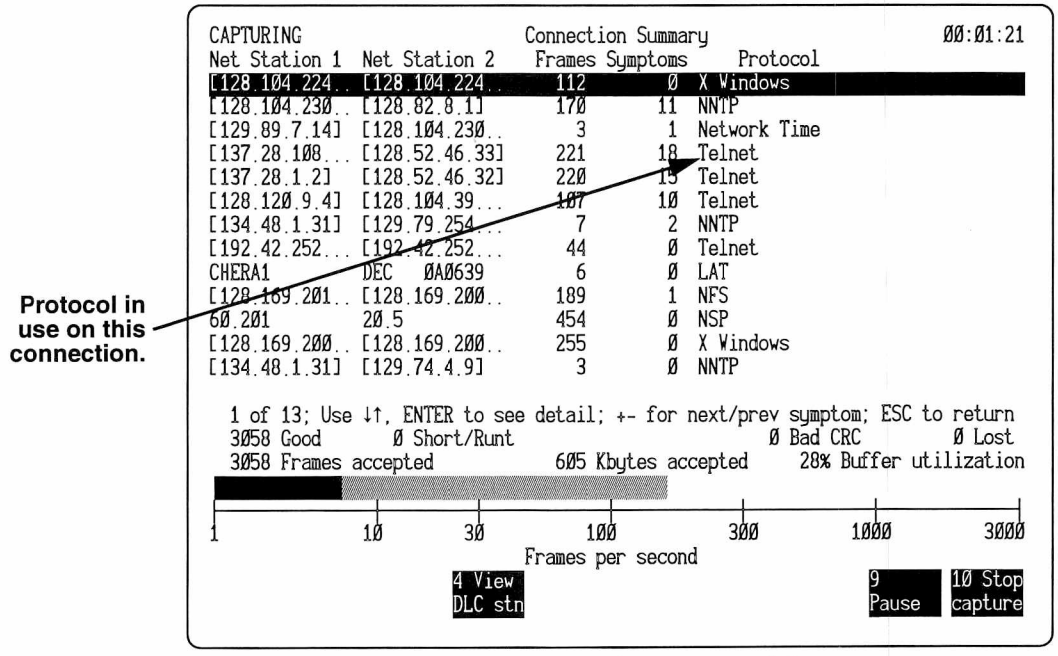

Protocol in use on this connection.
CAPTURING
Connection Summary
00:01:21
Net Station 1 Net Station 2 Frames Symptoms Protocol
[128.104.224.. [128.104.224.. 112 0 X Windows
[128.104.230.. [128.82.8.1] 170 11 NNTP
[129.89.7.14] [128.104.230.. 3 1 Network Time
[137.28.108... [128.52.46.33] 221 18 Telnet
[137.28.1.2] [128.52.46.32] 220 15 Telnet
[128.120.9.4] [128.104.39... 107 10 Telnet
[134.48.1.31] [129.79.254... 7 2 NNTP
[192.42.252... [192.42.252... 44 0 Telnet
CHERA1 DEC 0A0639 6 0 LAT
[128.169.201.. [128.169.200.. 189 1 NFS
60.201 20.5 454 0 NSP
[128.169.200.. [128.169.200.. 255 0 X Windows
[134.48.1.31] [129.74.4.9] 3 0 NNTP
1 of 13; Use ↓↑, ENTER to see detail; +- for next/prev symptom; ESC to return
3058 Good 0 Short/Runt 0 Bad CRC 0 Lost
3058 Frames accepted 605 Kbytes accepted 28% Buffer utilization
1
10
30
100
300
1000
3000
Frames per second
4 View DLC stn
9 Pause
10 Stop capture

Figure 5–31. Connection Summary window in Protocol format

Network Station Summary Window

Figure 5–32 shows the default format for the Network Station Summary window. The information fields found in the Network Station Summary window are described beginning on page 5–41.

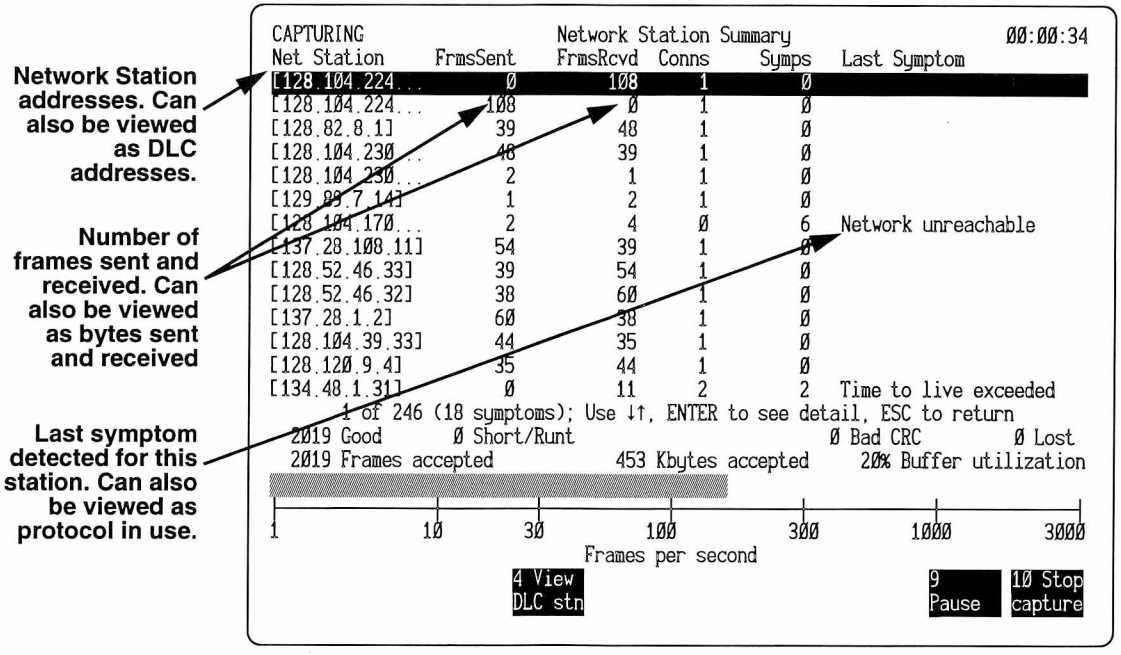

Network Station addresses. Can also be viewed as DLC addresses.
Number of frames sent and received. Can also be viewed as bytes sent and received
Last symptom detected for this station. Can also be viewed as protocol in use.
CAPTURING
Network Station Summary
00:00:34
Net Station FrmsSent FrmsRcvd Conns Symps Last Symptom
[128.104.224... 0 108 1 0
[128.104.224... 108 0 1 0
[128.82.8.1] 39 48 1 0
[128.104.230... 48 39 1 0
[128.104.230... 2 1 1 0
[129.88.7.14] 1 2 1 0
[128.104.170... 2 4 0 6 Network unreachable
[137.28.108.11] 54 39 1 0
[128.52.46.33] 39 54 1 0
[128.52.46.32] 38 60 1 0
[137.28.1.2] 60 38 1 0
[128.104.39.33] 44 35 1 0
[128.120.9.4] 35 44 1 0
[134.48.1.31] 0 11 2 2 Time to live exceeded
1 of 246 (18 symptoms); Use ↓↑, ENTER to see detail, ESC to return
2019 Good 0 Short/Runt 0 Bad CRC 0 Lost
2019 Frames accepted 453 Kbytes accepted 20% Buffer utilization
1 10 30 100 300 1000 3000
Frames per second
4 View DLC stn
9 Pause
10 Stop capture

Figure 5–32. Network Station Summary window

Figure 5-32 summarizes the available display formats for the Network Station Summary window.

Format	Column Entries					
Protocol Format	Net Station	Frames Sent	Frames Received	Connections	Symptoms	Protocol
Symptom Format	Net Station	Frames Sent	Frames Received	Connections	Symptoms	Last Symptom
DLC Station Format	DLC Station	Frames Sent	Frames Received	Connections	Symptoms	Last Symptom
Bytes Format	Net Station	Bytes Sent	Bytes Received	Connections	Symptoms	Last Symptom

Figure 5–33. Network Station layer Summary window formats

DLC Station Summary Window

Figure 5–34 shows the Protocol display format for the DLC Station Summary window. The information fields found in the DLC Station Summary window are described beginning on page 5–41.

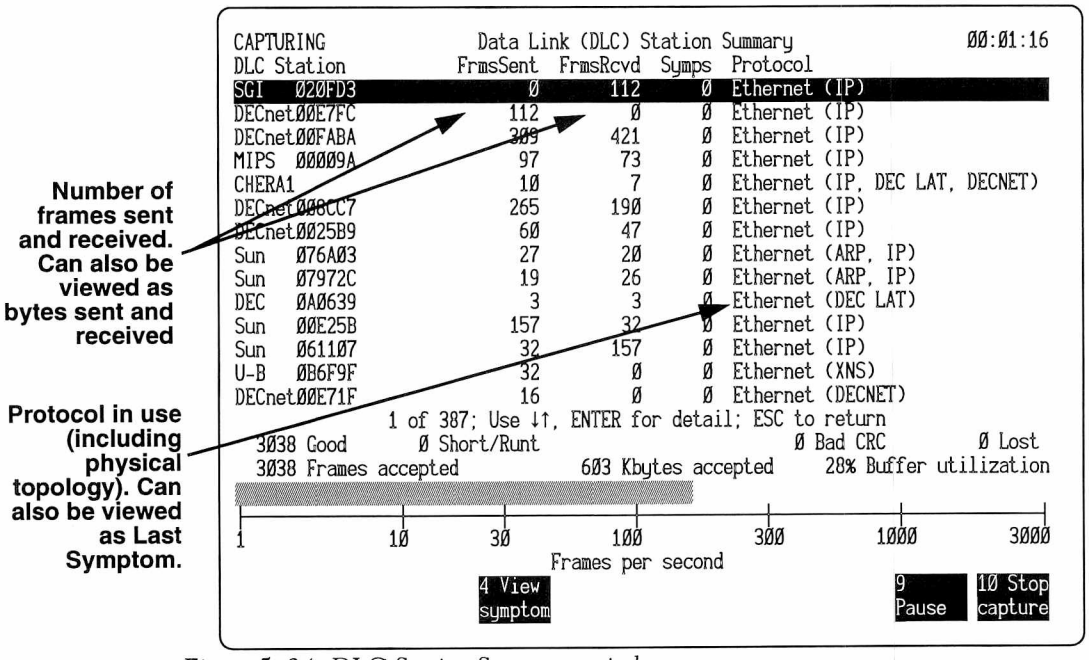

Number of frames sent and received. Can also be viewed as bytes sent and received
Protocol in use (including physical topology). Can also be viewed as Last Symptom.
CAPTURING
Data Link (DLC) Station Summary
00:01:16
DLC Station FrmsSent FrmsRcvd Symps Protocol
SGI 020FD3 0 112 0 Ethernet (IP)
DECnet00E7FC 112 0 0 Ethernet (IP)
DECnet00FABA 309 421 0 Ethernet (IP)
MIPS 00009A 97 73 0 Ethernet (IP)
CHERA1 10 7 0 Ethernet (IP, DEC LAT, DECNET)
DECnet008CC7 265 190 0 Ethernet (IP)
DECnet0025B9 60 47 0 Ethernet (IP)
Sun 076A03 27 20 0 Ethernet (ARP, IP)
Sun 07972C 19 26 0 Ethernet (ARP, IP)
DEC 0A0639 3 3 0 Ethernet (DEC LAT)
Sun 00E25B 157 32 0 Ethernet (IP)
Sun 061107 32 157 0 Ethernet (IP)
U-B 0B6F9F 32 0 0 Ethernet (XNS)
DECnet00E71F 16 0 0 Ethernet (DECNET)
1 of 387; Use ↓↑, ENTER for detail; ESC to return
3038 Good 0 Short/Runt 0 Bad CRC 0 Lost
3038 Frames accepted 603 Kbytes accepted 28% Buffer utilization
1 10 30 100 300 1000 3000
Frames per second
4 View symptom
9 Pause
10 Stop capture

Figure 5–34. DLC Station Summary window

The available display formats for the DLC Station Summary window are summarized in Figure 5–35.

Format	Column Entries				
Symptom Format	DLC Station	Frames Sent	Frames Received	Symptoms	Last Symptom
Bytes Format	DLC Station	Bytes Sent	Bytes Received	Symptoms	Last Symptom
Protocol Format	DLC Station	Frames Sent	Frames Received	Symptoms	Protocol

Figure 5–35. DLC Station Summary window formats

Subnet Pairs Summary Window

The Subnet Pairs Summary window lists all the pairs of communicating subnets detected by the Expert analyzer during its current capture session. The Expert analyzer learns about subnets by analyzing the information in the frames it captures. Symptoms are not categorized as occurring "at the subnet layer." The symptom counts in the Subnet Pairs Summary window refer to symptoms at all four Expert layers associated with the highlighted pair of subnets.

The Subnet Pairs Summary window (Figure 5–36) contains the following information:

Subnet 1	A subnet which the Expert analyzer learned about from routing information embedded in frames. When the analyzer learns the symbolic name of the subnet, it will substitute it for the hex address.
Subnet 2	Often the address of the subnet to which the Expert analyzer is attached. The analyzer provides the subnet address.
Frames	If there is a pair of subnets listed, the Frames count measures the total number of frames that have been transmitted between the two subnets. If there is only one subnet listed (instead of a pair), then the Frames count describes the activity internal to that subnet.
Hops	The hop count between the two subnets. If the hop count is zero, it indicates either a local subnet or that no Routing Information Protocol (RIP) packets have been seen.
Symptoms	The total number of symptoms associated with traffic between these two subnets at the Expert Application and Connection layers. A subnet that has a high ratio of symptoms to packets is likely to have some kind of problem, or an area in which operation can be made more efficient.
Protocol	The protocol in use on Subnet 1.

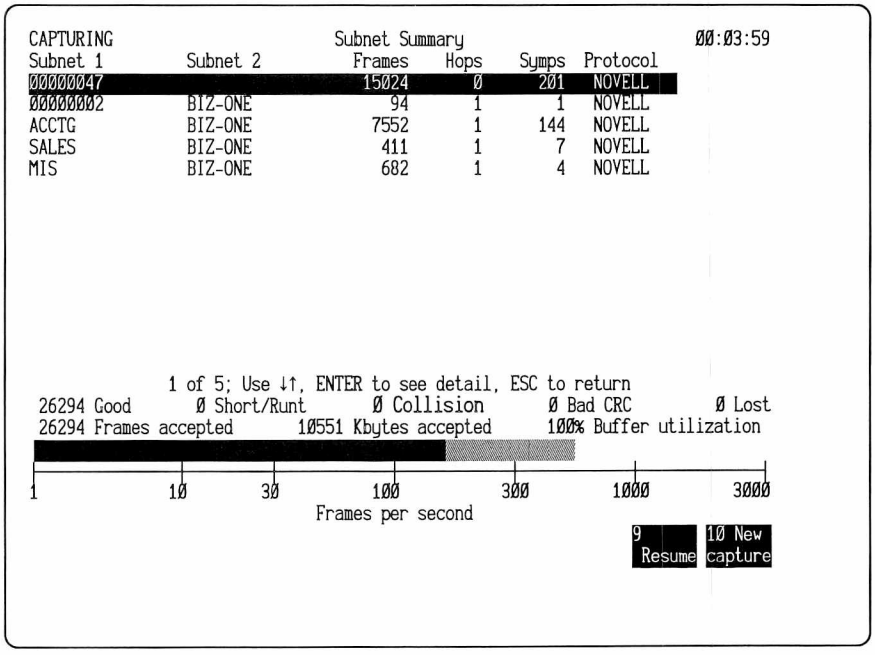

CAPTURING
Subnet Summary
ØØ:Ø3:59
Subnet 1 Subnet 2 Frames Hops Symps Protocol
ØØØØØØ47 15Ø24 Ø 2Ø1 NOVELL
ØØØØØØØ2 BIZ-ONE 94 1 1 NOVELL
ACCTG BIZ-ONE 7552 1 144 NOVELL
SALES BIZ-ONE 411 1 7 NOVELL
MIS BIZ-ONE 682 1 4 NOVELL
1 of 5; Use ↓↑, ENTER to see detail, ESC to return
26294 Good Ø Short/Runt Ø Collision Ø Bad CRC Ø Lost
26294 Frames accepted 1Ø551 Kbytes accepted 1ØØ% Buffer utilization
1 1Ø 3Ø 1ØØ 3ØØ 1ØØØ 3ØØØ
Frames per second
9 Resume
1Ø New capture

Figure 5–36. Subnet Pairs Summary window

Global Symptom Summary Window

The Global Symptom Summary window provides information on global symptoms detected by the Expert analyzer during its current capture session.

Global symptoms include, but are not limited to:

- Network Overload
- Broadcast/Multicast Storm
- WAN Underload

Figure 5–37 shows the Global Symptom Summary window.

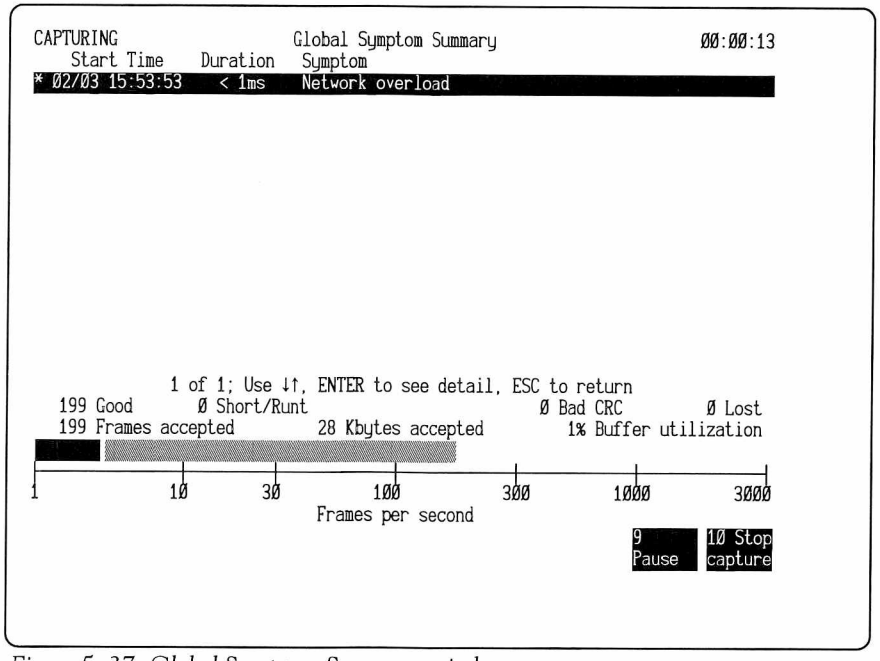


Figure 5–37. Global Symptom Summary window

The Global Symptom Summary window contains the following information:

Start Time	The time and date at which the symptom was first detected by the analyzer.
Duration	The length of time (in milliseconds) during which the symptom was valid. If there is an asterisk in the far left column, as in Figure 5–37, the symptom is still active.
Symptom	A one-line description of the symptom detected.

You can control when the analyzer generates Network Overload symptoms and diagnoses by setting the **LAN Overload** and **LAN Overload %** thresholds in the **Expert config\Thresholds\DLC Station** menu. Similarly, WAN Overload symptoms and diagnoses are controlled by the **WAN Overload Timer** and **WAN Overload %** thresholds. Broadcast/Multicast storm symptoms and diagnoses are controlled by the **Broadcast sy** and **Broadcast dg** thresholds. For information on Expert thresholds, refer to "Setting Thresholds for Symptoms and Diagnoses" on page 4–13.

Symptom and Network Object Detail Windows

The Symptom and Network Object Detail windows provide specific information about particular connections, network stations, or DLC stations. Figure 5–38 shows the Detail window for a connection between the NetWare server BIZ-ONE and the workstation AGNES at the Application layer. The analyzer provides the DLC and network addresses of the endpoints of the connection, the protocol in use, and a list of all the symptoms associated with this connection. At this point, you would probably pause capture by pressing F9 **[Pause]**, and press F1 **[Explain]** to read the context-sensitive Explain message associated with these symptoms.

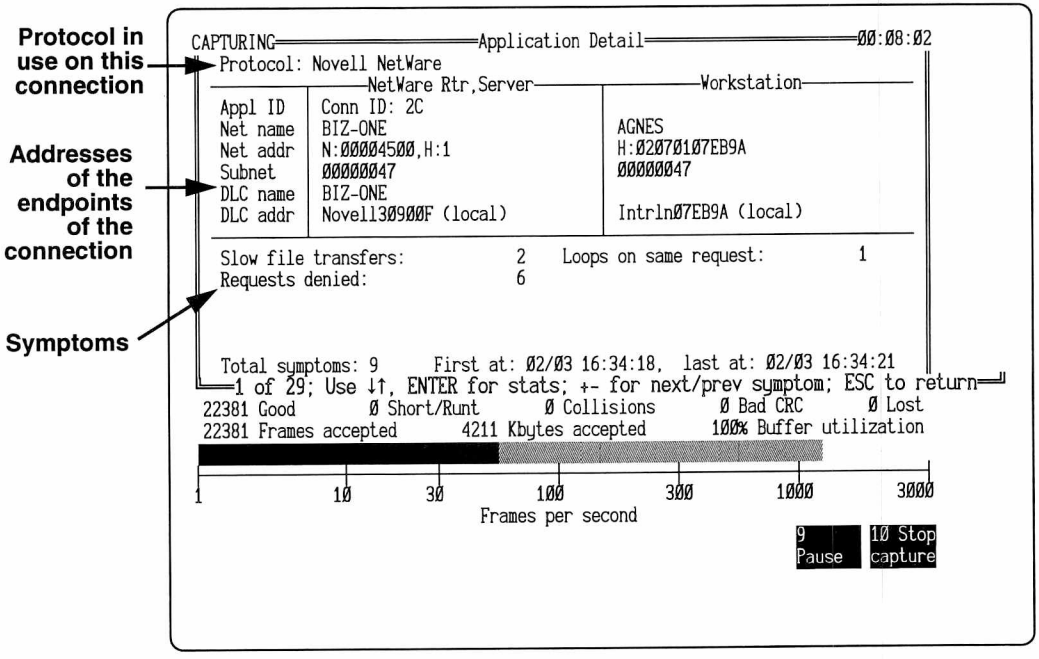


Figure 5–38. Application Detail window

Displaying the Detail Window

There are two ways to display the Detail window:

- From the Symptom and Network Object column of the Expert Overview
- From the Diagnoses column of the Expert Overview

To display a Detail window from the Symptom and Network Object column of the Expert Overview:

1. In the Symptom and Network Object column, use the cursor keys to highlight the Expert layer containing the connection, network station, or DLC station in which you are interested.
2. Press ENTER.

   Result: The Summary window for the selected Expert layer appears.
3. Use the cursor keys to highlight the desired connection, network station, or DLC station in the Summary window.
4. Press ENTER.

   Result: A Detail window similar to Figure 5–38 appears. The exact format of the Detail window depends on the layer selected and the number of symptoms detected.

You can also display a Symptom and Network Object Detail window from the Diagnoses column of the Expert Overview.

To display a Symptom and Network Object Detail window from the Diagnoses column of the Expert Overview:

1. In the Diagnoses column of the Expert Overview, use the cursor keys to highlight an Expert layer containing at least one diagnosis.
2. Press ENTER.

   Result: The Diagnosis Summary for the selected layer appears.
3. Use the cursor keys to highlight the desired diagnosis and press ENTER.

   Result: The Diagnosis Detail window appears. (The Diagnosis Detail window is different from the Symptom and Network Object Detail window. The Diagnosis Detail window provides specific information on a diagnosis, while the Detail window provides more general information such as network addresses, DLC addresses, and symptoms detected.)
4. Press ENTER.

   Result: The Detail window for the connection, network station, or DLC station associated with the selected diagnosis appears. Figure 5–38 is an example of a Detail window.

NOTE: From the Diagnoses column of the Expert Overview, you cannot display the Subnet Pairs or the Global Symptom Detail windows. These windows can only be displayed from the Symptom and Network Object column of the Expert Overview.

From the Symptom and Network Object column of the Expert Overview, you can use the cursor keys to scroll through the Detail windows for each connection, network

station, or DLC station listed in the Summary display (from the Diagnoses column of the Expert Overview, you cannot). When you return to the Summary window from the Detail windows, the analyzer will automatically highlight the connection or address associated with the Detail display from which you came.

Information in the Detail Windows

The information presented in the Detail windows is very similar at each of the four Expert layers. However, the Subnet Pairs and Global Symptom Detail windows are somewhat different. Those windows are described in later sections.

The Detail windows for the Network Station and DLC layers contain less information than those at the Application and Connection layers. This is because the analyzer detects information for single stations at the Network Station and DLC layers, while at the Application and Connection layers it detects information about connections between two stations. This means that there is twice as much address information to present in the Detail window for the Application and Connection layers.

Figure 5–39 is an example of a Detail window at the Network Station layer. Notice that the information presented is the same as in Figure 5–38 but for only one station.

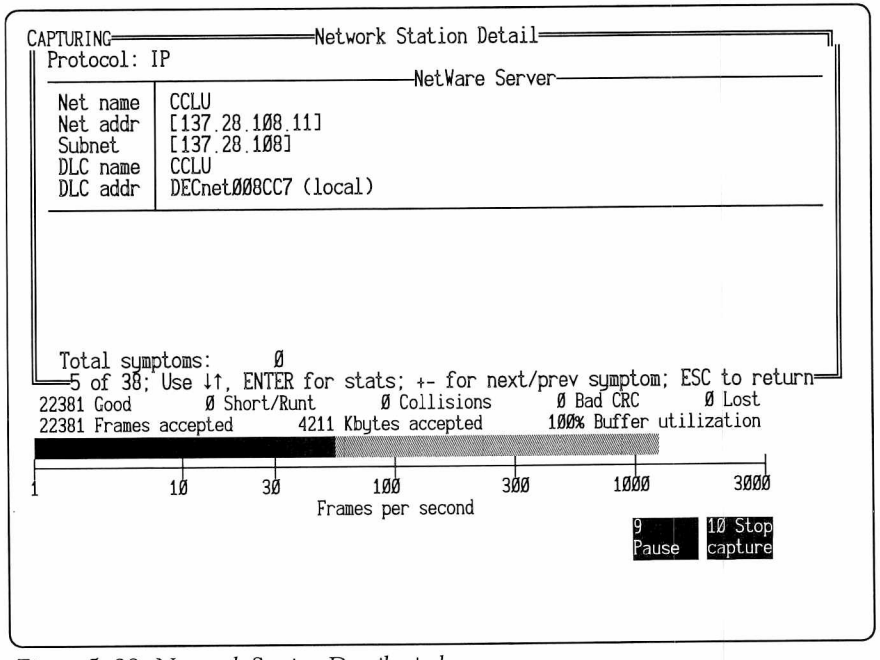


Figure 5–39. Network Station Detail window

The list below summarizes the information found in the Detail windows. Not all the information is found in every screen. The exact information in the Detail display depends on the Expert layer and the object highlighted.

Protocol — The protocol in use on this connection. If the analyzer does not recognize the protocol in use, it will substitute the well-known port name (which is usually also a protocol name, such as Telnet or FTP).

Appl ID — The application ID for this connection. Most protocols use an identification scheme to give unique names to connections between network stations. The Expert analyzer learns the identification scheme for the particular protocol involved and displays that information.

For example, TCP uses Port numbers, DECnet uses Logical link numbers, and Novell uses Connection IDs. The Expert analyzer displays the identification scheme appropriate to the protocol in use.

Net name — The symbolic name for this station. This field will remain blank until the analyzer learns the symbolic name.

Net addr — The network address of this station.

Subnet — The subnet on which this station resides.

DLC name — The symbolic DLC name for this station. This field will remain blank until the analyzer learns the symbolic name.

DLC addr — The DLC address for this station. The analyzer automatically attempts to interpret the first three bytes of the address as the name of the NIC's manufacturer. When it is able to find the manufacturer's code in its table of manufacturers, the analyzer replaces the first three bytes of the station address with an ASCII abbreviation of the manufacturer's name.

The DLC address of a station may be different than the network station address. This occurs when the analyzer captures frames from a remote station. The analyzer will show the DLC address of the router rather than that of the originating station. When this occurs, the DLC address will be followed by the message `(remote routed)`. Figure 5–40 shows how this can happen.

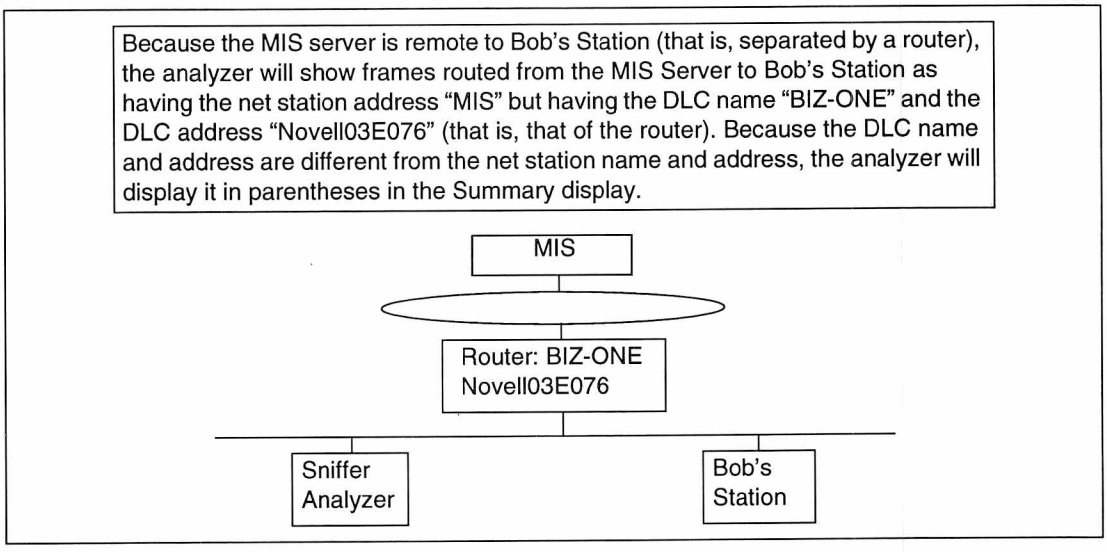

Because the MIS server is remote to Bob's Station (that is, separated by a router), the analyzer will show frames routed from the MIS Server to Bob's Station as having the net station address "MIS" but having the DLC name "BIZ-ONE" and the DLC address "Novell03E076" (that is, that of the router). Because the DLC name and address are different from the net station name and address, the analyzer will display it in parentheses in the Summary display.
MIS
Router: BIZ-ONE
Novell03E076
Sniffer
Analyzer
Bob's
Station

Figure 5–40. How the analyzer interprets the DLC name and address of remote stations

Total symptoms — Total number of symptoms associated with this connection or station. The Detail window also lists each symptom associated with the selected connection or station, followed by a dynamic counter.

Detail windows will often include a short message about a particular symptom detected by the analyzer. For more information on these messages, press F1 **[Explain]** to invoke the Explain message pertinent to the current display.

Subnet Pairs Detail Window

The Subnet Pairs Detail window displays the number of packets transferred between two subnets and the number of symptoms (at the Connection and Application Expert layers) associated with those packets. The symptoms are presented with an individual counter for each Expert layer.

Additionally, the Detail window lists any routers used to access the subnet on which the Expert analyzer is not attached. The hop count is included. Figure 5–41 is an example of a Subnet Pairs Detail window.

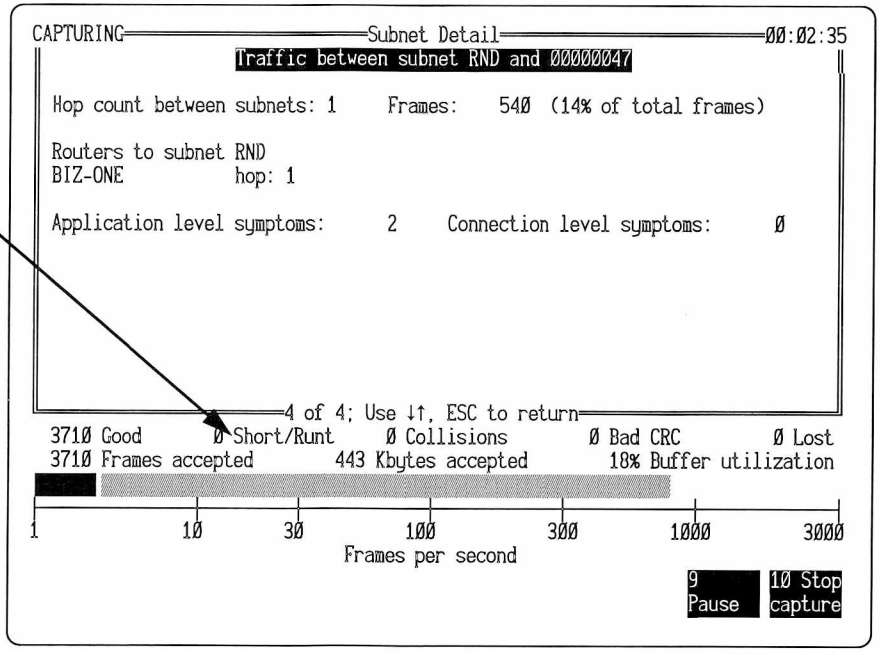


Figure 5–41. Subnet Pairs Detail Window

The list below describes the information in the Subnet Detail window:

Hop count between subnets	Lists the number of hops between these two subnets.
Frames	Lists the number of frames exchanged at the Expert Connection layer. The % **of total frames** counter is the ratio between the number of frames exchanged at the Expert Connection layer and the total number of frames exchanged at all layers. This gives you an idea of the "useful" traffic on your network.
Routers to subnet	Lists the routers used to access the subnet.
Symptoms	Lists the number of symptoms detected at the Application and Connection Expert layers.

The information in the Subnet Pairs Detail window varies according to the protocol in use. For example, Figure 5–41 shows the Subnet Pairs Detail window for a pair of communicating Novell subnets. The Subnet Pairs Detail window for a DECnet network includes protocol-specific information, such as DECnet areas. TCP/IP Subnet Pairs Detail windows are similar to the Novell window. However, you should

know how to define the subnet mask for the various TCP/IP networks to which you will attach the Expert analyzer. See "Setting Subnet Masks" on page 4–7 for more information on defining the subnet mask.

You display the Subnet Pairs Detail window in the same way you display any Detail window. See "To change the format of the Summary window:" on page 5–43.

NOTE: One of the entries in the Subnet Summary window will not list a pair of communicating subnets. That is the entry for the subnet to which the Sniffer Network Analyzer is attached. Its Detail window will measure frames and symptoms for its specific subnet alone.

Global Symptom Detail Window

The Global Symptom Detail window provides specific information on certain global symptoms. Global symptoms include:

- LAN Overload
- Broadcast/Multicast Storm
- WAN Overload
- WAN Underload

You can control when these symptoms are generated by adjusting the Expert thresholds. For more information on Expert thresholds, see "Setting Thresholds for Symptoms and Diagnoses" on page 4–13.

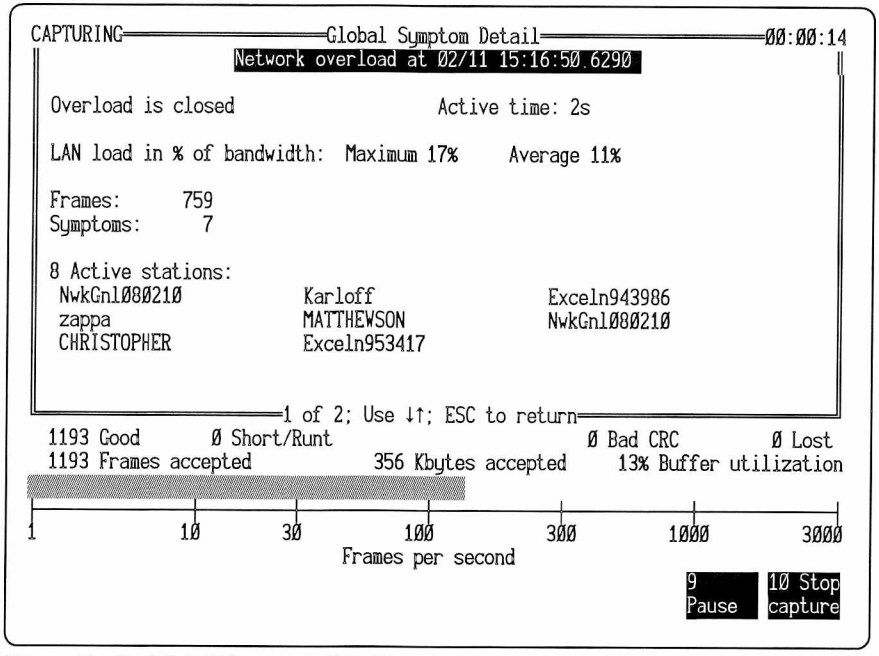


Figure 5–42. Global Symptom Detail window

The Global Symptom Detail window (Figure 5–42) is displayed in the same way you display any Detail window. For more information, see "To display a Summary window at any of the Expert layers:" on page 5–39.

Information in the Global Symptom Detail Window

The list below summarizes the information found in the Global Symptom Detail Window:

Active time	Length of time for which the LAN Overload or Broadcast/Multicast storm symptom was active.
State	Current status of the named symptom. Status is either closed or active.
Max load %	Maximum network load during the time the named symptom was active. Measured as a percentage of available bandwidth, where available bandwidth is the theoretical maximum of the medium in use (for example, 10 Mbps is the theoretical maximum for Ethernet).
Average load %	Average network load during the time the named symptom was active. Measured as percentage of available bandwidth (see **Max load %**, above).
Broadcasts	Number of broadcast frames detected.
Active stations	Number of active stations transmitting during the time the LAN Overload or Broadcast\Multicast storm symptom was active. The stations are listed by address or symbolic name.
Frames	Total number of frames associated with the highlighted overload.
Symptoms	Total number of symptoms associated with frames associated with highlighted overload.

Symptom and Network Object Statistics Windows

Statistics windows provide in-depth statistics relating to a selected application, connection, network station, or DLC station. Statistics windows provide information on topics such as average file performance, number of frames sent, and the number of connections for a given station. The exact information depends on the layer for which the Statistics window is displayed and the protocol in use.

The following sections describe the Statistics windows for each of the following Expert layers:

- Application

- Connection
- Network Station
- DLC Station

NOTE: There are no Statistics windows associated with the Subnet Pairs or Global Symptom screens.

Displaying a Statistics Window

There are two ways to display a Statistics window:

- From the Symptom and Network Object column of the Expert Overview
- From the Diagnoses column of the Expert Overview

To display a Statistics window from the Symptom and Network Object column of the Expert Overview:

1. In the Symptom and Network Object column of the Expert Overview, display the Summary window for the Expert layer containing the connection, network station or DLC station in which you are interested.
2. From the Summary window, display the Detail window for the desired connection, network station, or DLC station.
3. Press ENTER.

   Result: A Statistics window like Figure 5–43 appears. The exact format of the Statistics window depends on the layer selected, the protocol in use, and the number of symptoms detected.

You can also display a Statistics window from the Diagnoses column of the Expert Overview.

To display a Statistics window from the Diagnoses column of the Expert Overview:

1. In the Diagnoses column of the Expert Overview, use the cursor keys to highlight an Expert layer containing at least one diagnosis.
2. Press ENTER.

   Result: The Diagnosis Summary for the selected layer appears.
3. Use the cursor keys to highlight the desired diagnosis and press ENTER.

   Result: The Diagnosis Detail window appears.
4. Press ENTER.

   Result: The Detail window associated with the selected diagnosis appears. (This Detail window is different from the Diagnosis Detail window.)

5. Press ENTER.

   Result: The Statistics window associated with the selected diagnosis appears. Figure 5–43 shows a Statistics window at the Application layer.

Figure 5–1 summarizes the relationships between the various Expert windows.

Application Statistics Window

The Application Statistics window provides statistics related to specific connections detected at the Application layer. Figure 5–43 is an example of the Statistics window for an Application layer connection between the server BIZ-ONE and the workstation MajorDomo.

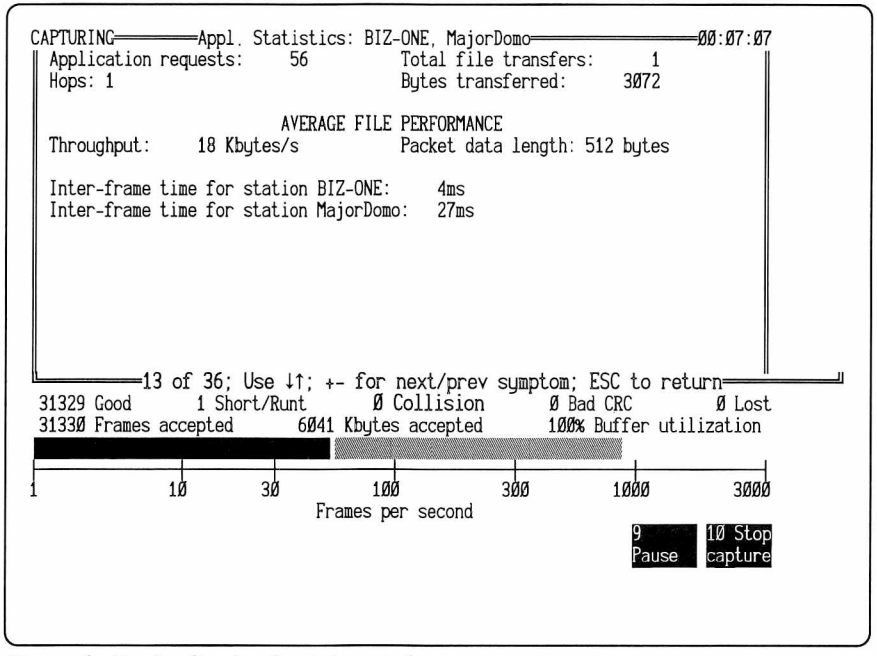


Figure 5–43. Application Statistics window

The Application Statistics window provides the following statistics:

Application requests	The number of file requests detected for this connection.
Total file transfers	The number of file regions transferred on this connection.
Hops	The number of hops between the endpoints of this connection.
Bytes transferred	The number of bytes transferred on this connection.

If the analyzer has detected at least one file transferred on a given connection, the Statistics window will also contain statistics on average file performance. Average file performance statistics include:

Throughput	Measures the average speed at which data was transferred between the two stations. Units are in Kbytes/s.
Packet data length	Average length of data packets on this connection. Units are in bytes.
Interframe time for station	Average response time for a given station. With a request/reply protocol such as Novell PEP, the Interframe time is simply the average of the delta times between the time a station receives a request and the time it sends a reply. In a windowing protocol, such as TCP/IP, or DECnet, the Interframe time is the average of both the delta time between when a station receives a request and sends a reply and the delta times between replies to a single file request. Figure 5–44 summarizes how Interframe time is calculated for both types of protocols.

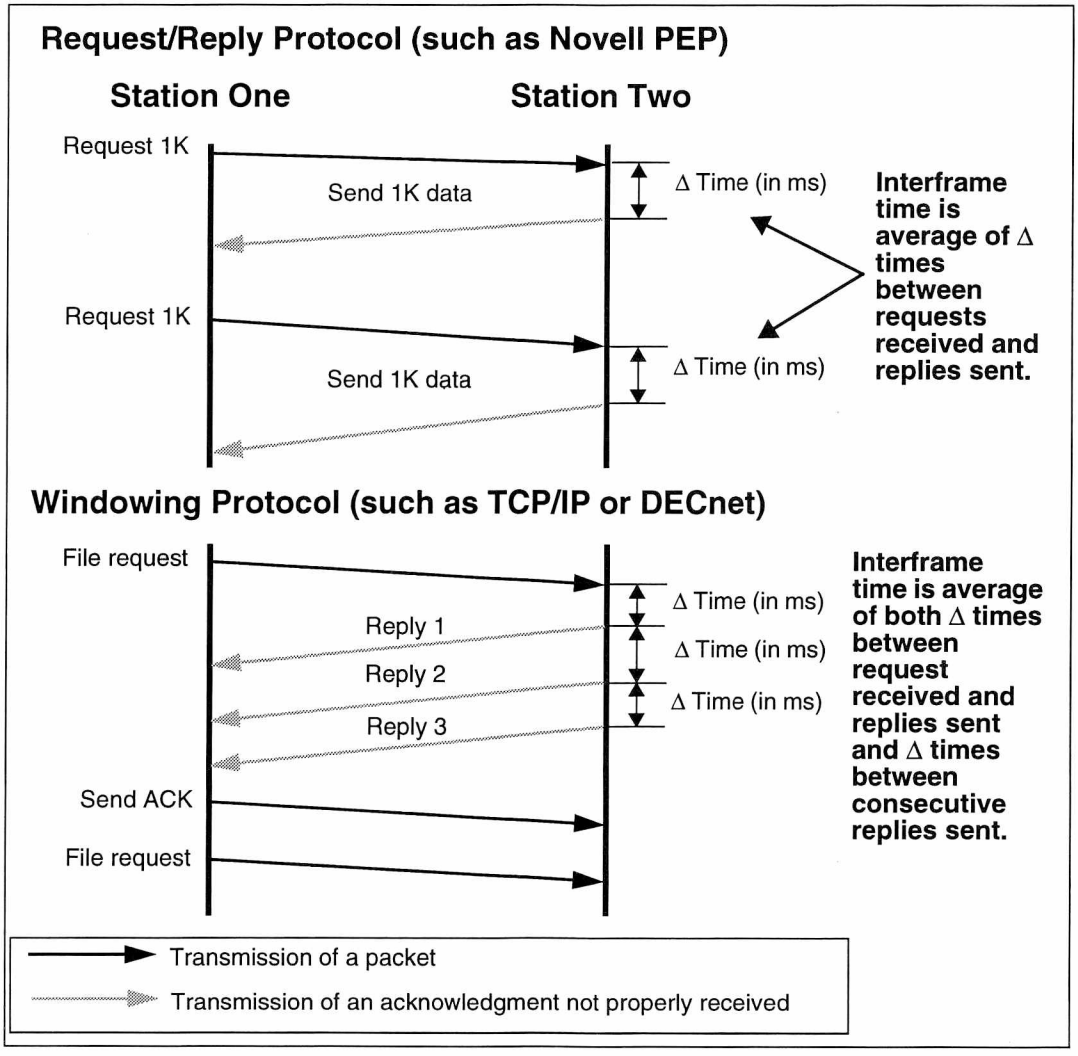

Request/Reply Protocol (such as Novell PEP)
Station One
Station Two
Request 1K
Send 1K data
Δ Time (in ms)
Interframe time is average of Δ times between requests received and replies sent.
Request 1K
Send 1K data
Δ Time (in ms)
Windowing Protocol (such as TCP/IP or DECnet)
File request
Reply 1
Reply 2
Reply 3
Δ Time (in ms)
Δ Time (in ms)
Δ Time (in ms)
Interframe time is average of both Δ times between request received and replies sent and Δ times between consecutive replies sent.
Send ACK
File request
Transmission of a packet
Transmission of an acknowledgment not properly received

Figure 5–44. How the Expert analyzer calculates the value for Interframe time

Connection Statistics Window

The Connection Statistics window provides information on specific connections detected at the Connections layer. The exact information in the Statistics window depends on the protocol in use. Figure 5–45 shows the Statistics window for a connection using the TCP/IP protocol.

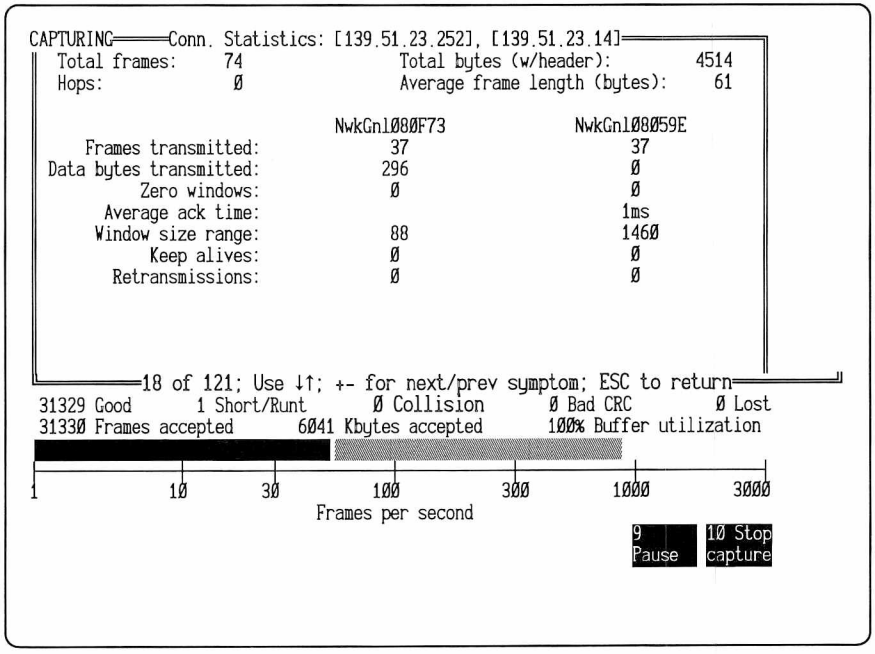

CAPTURING
Conn. Statistics: [139.51.23.252], [139.51.23.14]
Total frames: 74
Total bytes (w/header): 4514
Hops: 0
Average frame length (bytes): 61
NwkGnl080F73
NwkGnl08059E
Frames transmitted: 37 37
Data bytes transmitted: 296 0
Zero windows: 0 0
Average ack time: 1ms
Window size range: 88 1460
Keep alives: 0 0
Retransmissions: 0 0
18 of 121; Use ↓↑; +- for next/prev symptom; ESC to return
31329 Good 1 Short/Runt 0 Collision 0 Bad CRC 0 Lost
31330 Frames accepted 6041 Kbytes accepted 100% Buffer utilization
1 10 30 100 300 1000 3000
Frames per second
9 Pause
10 Stop capture

Figure 5–45. Connection Statistics window (in this case, for TCP/IP)

The following information is found in the Connection Statistics window regardless of the protocol used:

Total frames	Total number of frames transmitted on this connection.
Total bytes	Total number of bytes transferred on this connection. This number includes the headers of all frames transmitted.
Hops	The number of hops between the endpoints of this connection.
Average frame length	The average length of the frames transmitted on this connection. Units are in bytes.

The Connection Statistics window also provides protocol-specific statistics. Figure 5–45 shows the statistics provided for a TCP/IP connection. For an explanation of these and other protocol-specific statistics, pause the capture and press F1 **[Explain]**.

Network Station Statistics Window

The Network Station Statistics window provides statistics for individual network stations. The counters in Figure 5–46 are the same as those in the Connection Statistics window in Figure 5–45. However, in the Network Station window, these counters pertain to the highlighted station alone, rather than a connection. The list below summarizes the information found in the Network Station Statistics window.

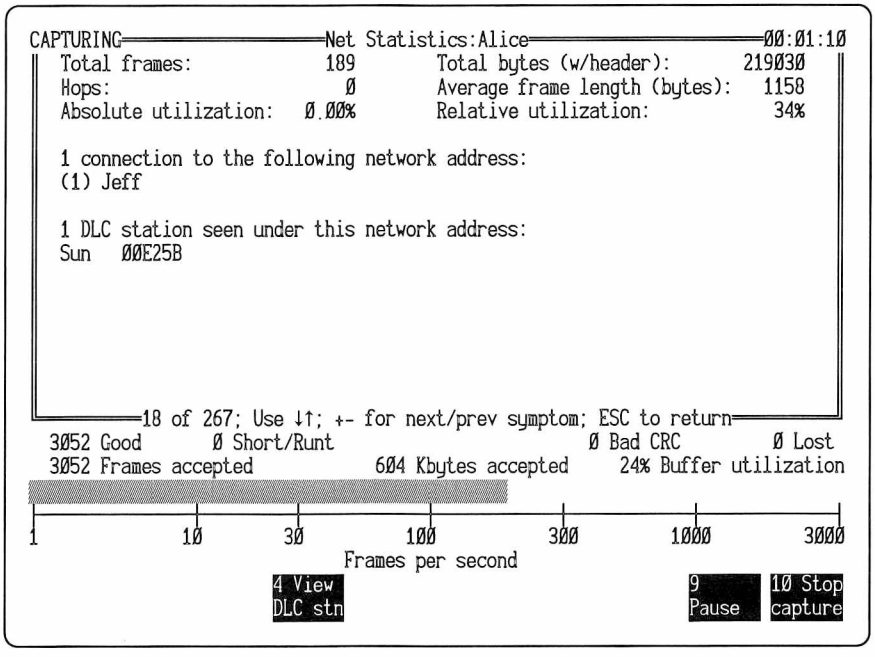


Figure 5–46. Network Station Statistics window

Total frames	Total number of frames transmitted and received by this station.
Total bytes	Total number of bytes transmitted and received by this station. This number includes the headers of all frames.
Hops	Total number of hops associated with frames sent and received by this station.
Average frame length	The average length of all frames transmitted and received by this station. Units are in bytes.

Absolute utilization	Network utilization for this DLC station computed as a percentage of maximum theoretical available bandwidth. For example, the theoretical maximum available bandwidth for Ethernet is 10 Mbps. Absolute utilization is updated every second and is measured over the time period since the first frame of the current capture session was passed into the capture buffer.
Relative utilization	Network utilization for this DLC station computed as a percentage of traffic seen by the analyzer. For example, if the analyzer has seen 100 bytes of traffic and Station A has sent 50 of them, then Station A's relative utilization is 50 percent.
Connections to net stations	The Statistics window lists all DLC stations to which the highlighted station has connected, as well as a counter of how many times. In Figure 5–46, the network station Alice has connected to the DLC station Jeff once.
Associated DLC addresses	The Statistics window provides the DLC addresses of stations associated with the selected network station (see below).

If frames have been routed from a remote network segment, the two stations may not be the same. In that case, the associated DLC station would probably be the router or server through which the frames were routed. If this is the case, the hop count will be greater than one, indicating that frames have been remote routed. Then, the DLC station address will probably be different from the network station address.

DLC Station Statistics Window

Just as the Network Station Statistics window provides statistics for network stations, the DLC Station Statistics window provides statistics for DLC stations. Figure 5–47 shows the DLC Station Statistics window for the DLC station BIZ-ONE.

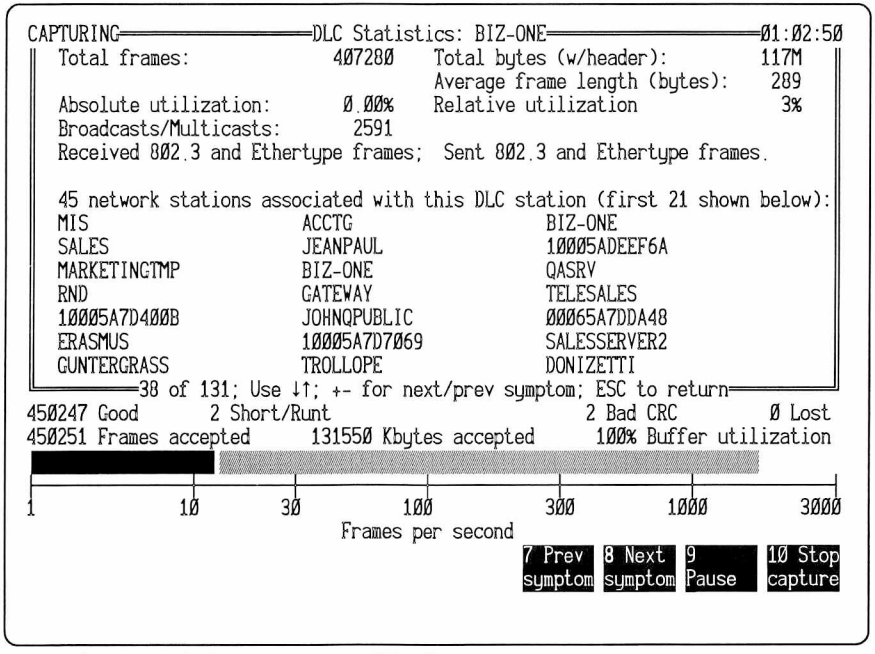

CAPTURING
DLC Statistics: BIZ-ONE
01:02:50
Total frames: 407280
Total bytes (w/header): 117M
Average frame length (bytes): 289
Absolute utilization: 0.00%
Relative utilization 3%
Broadcasts/Multicasts: 2591
Received 802.3 and Ethertype frames; Sent 802.3 and Ethertype frames.
45 network stations associated with this DLC station (first 21 shown below):
MIS ACCTG BIZ-ONE
SALES JEANPAUL 10005ADEEF6A
MARKETINGTMP BIZ-ONE QASRV
RND GATEWAY TELESALES
10005A7D400B JOHNQPUBLIC 00065A7DDA48
ERASMUS 10005A7D7069 SALESSERVER2
GUNTERGRASS TROLLOPE DONIZETTI
38 of 131; Use ↓↑; +- for next/prev symptom; ESC to return
450247 Good 2 Short/Runt 2 Bad CRC 0 Lost
450251 Frames accepted 131550 Kbytes accepted 100% Buffer utilization
1 10 30 100 300 1000 3000
Frames per second
7 Prev symptom
8 Next symptom
9 Pause
10 Stop capture

Figure 5–47. DLC Station Statistics Window

The DLC Station Statistics window is very similar to the Network Station Statistics window, inasmuch as it contains several of the same counters. These counters include:

- Total frames
- Total bytes
- Average frame length

However, the DLC Station Statistics window also provides the following information:

Absolute utilization	Network utilization for this DLC station computed as a percentage of maximum theoretical available bandwidth. For example, the theoretical maximum available bandwidth for Ethernet is 10 Mbps. Absolute utilization is updated every second and is measured over the time period since the first frame of the current capture session was passed into the capture buffer.
Broadcasts/Multicasts	Number of broadcast/multicast frames sent and received.

Received/Sent	On an Ethernet network, the Statistics window describes the type of Ethernet frames sent and received by the highlighted station. In Figure 5–47, the DLC station, "BIZ-ONE," sent and received 802.3 and other Ethertype frames.
Relative utilization	Network utilization for this DLC station computed as a percentage of traffic seen by the analyzer. For example, if the analyzer has seen 100 bytes of traffic and Station A has sent 50 of them, then Station A's relative utilization is 50 percent.
Associated network stations	This field lists up to the first 21 network station addresses with which the highlighted DLC station address is associated. If there are more than 21 stations, the analyzer generates the message, "xx network stations associated with this DLC station (first 21 shown below)." In Figure 5–47, since the DLC station, "BIZ-ONE," is a server, it transfers data for many network stations (leading its DLC address to be associated with a multitude of network station addresses. For an illustration of this concept, see Figure 5–40 on page 5–56). However, if the highlighted DLC station were a workstation, the **Associated network stations** list would probably include only the workstation itself.

Additional Token Ring Counters in the DLC Station Statistics Window

On token ring, the DLC Station Statistics window provides the following additional information:

Station status — This field tells you whether the highlighted station is currently ON RING or OFF RING.

Upstream neighbor — Identifies the highlighted station's upstream neighbor by address or symbolic name.

Additionally, the DLC Stations Statistics window tabulates ring purge frames and informs you if the highlighted station is the active monitor.

The Global Statistics Window

The Global Statistics window provides a comprehensive percentage breakdown by protocol family of the traffic found on your network, as well as information about the current capture session. The information in the Global Statistics window is not immediately related to the investigation of symptoms and diagnoses; however, it does provide valuable insight on the types of traffic found on your network. Figure 5–48 shows the Global Statistics window for an Ethernet network.

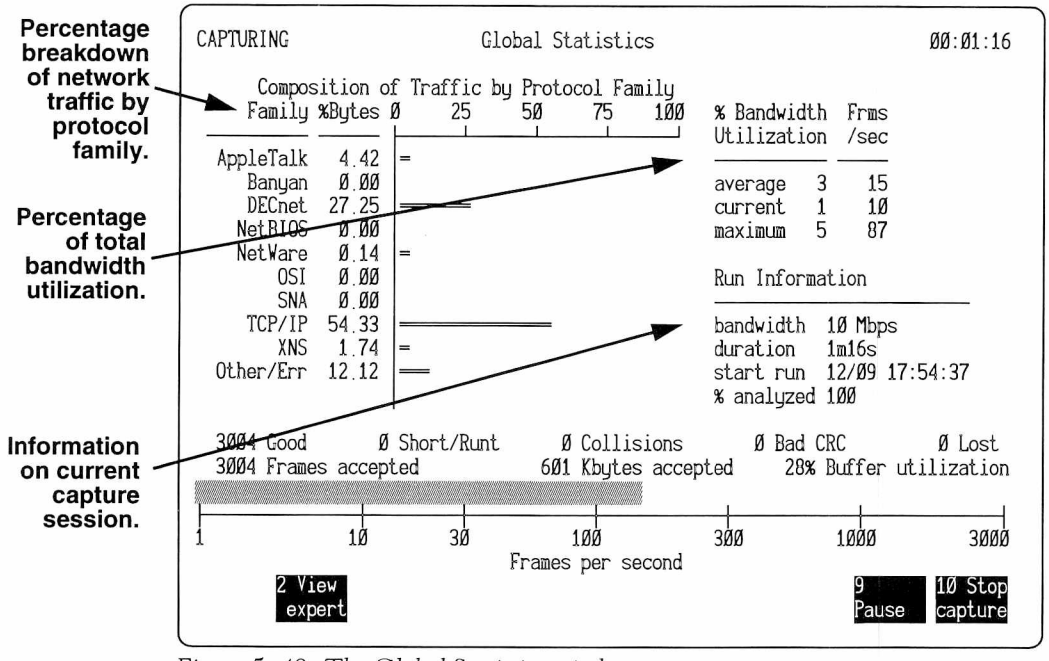


Figure 5–48. The Global Statistics window

The Global Statistics window is always available from the Expert Overview by using the F2 key. However, you cannot display the Global Statistics window from the various Expert subdisplays.

To display the Global Statistics window:

1. In the Expert Overview, press F2 **[View stats]**.

   Result: The Global Statistics window appears, as in Figure 5–48.

   After displaying the Global Statistics window, the function key label for F2 changes from **View stats** to **View expert**. You can use this key to toggle between the two views.

Composition of the Global Statistics Window

The Global Statistics Window consists of three categories of information:

- Composition of Traffic by Protocol Family
- Bandwidth Utilization
- Run Information

Each of these three categories is visible in Figure 5–48 and is described below.

Composition of Traffic by Protocol Family

The Expert analyzer dynamically tabulates all network traffic according to its protocol family. The results are presented both graphically (as a histogram) and as a numeric percentage. The thermometer-style horizontal bar allows you to see at a glance which count is increasing. The exact percentage of total traffic is displayed at the left end of the bar. For example, in Figure 5–48, TCP/IP traffic accounts for 54.33 percent of all network traffic, while AppleTalk accounts for only 4.42 percent.

How the Expert Analyzer Categorizes Packets into Protocol Families

In compiling the histogram, the expert system counts all the bytes in all the frames, except for the following.

1. Frames excluded by the capture filters.
2. Frames that arrive while capture is paused.
3. Frames that are skipped because the expert analysis is unable to keep up with the influx of frames (in this case the "% analyzed" statistic, described below, will be less than 100%).
4. Internetwork analyzer only: FCS bytes, flag bytes and bits inserted by the bit-stuffing process.

Each frame is categorized into one of the protocol families listed at the left of the histogram. If none of the listed protocols apply, a frame is categorized as "Other/Err". Frames with collisions or CRC errors are also included in "Other/Err". If more than one protocol applies, a frame is categorized according to the highest protocol analyzed.

For example, on a Frame Relay link, all traffic can technically be considered to be Frame Relay. However, encapsulated within most of these Frame Relay packets are LAN packets with higher-level protocols– for example, IP. The Expert analyzer would categorize all bytes in a Frame Relay packet with an encapsulated IP layer as part of the TCP/IP family. The only Frame Relay packets that the analyzer would categorize into the Frame Relay protocol family would be LMI frames, such as FECN and BECN frames. This convention lets you answer questions such as, "By how much would traffic be reduced if we removed all the TCP/IP stations from this network segment."

The expert system does not always parse to the highest layer of a frame. For example, the current software release will not recognize an AppleTalk frame that is encapsulated in a TCP/IP frame. Therefore, it will categorize such a frame as TCP/IP rather than AppleTalk.

"Protocol Family" is a generic term for a related set of protocols. For example, the TCP/IP protocol family counter in the Global Statistics screen tabulates all protocols with an IP layer– not just TCP over IP. The other Protocol Families operate similarly.

Percentage Bandwidth Utilization

This category of counters measures the average, current, and maximum percentage of bandwidth used during the current capture session. **Current bandwidth usage** is measured over the interval of one second, on a "sliding-window" basis. That is, a new measurement is made every tenth of a second over the interval of one second (that is, measurements would be made from 1.0 to 2.0 seconds, from 1.1 to 2.1 seconds, and so on). **Maximum percentage of bandwidth** is the largest of these "current" bandwidth usage values. **Average bandwidth usage** is calculated by counting all frames that have entered the buffer since the start of the current capture and dividing this value by the total number of seconds the analyzer has been capturing frames (not paused).

NOTE: Although the analyzer makes many measurements per second, the counters are updated only once every second.

On the Sniffer Internetwork Analyzer (the Sniffer analyzer for WAN/Synchronous), the counts for percentage bandwidth utilization are expanded to measure **From DTE** and **From DCE** separately.

The **From DTE** and **From DCE** percentage bandwidth utilization counters are separate from one another. That is, they do not need to add up to 100 percent. Each WAN link consists essentially of two separate pipes with traffic travelling in opposite directions. Since each "pipe" is independent of the other, percentage bandwidth utilization could theoretically go to 100 percent for either one.

Additionally, there are statistics for average, current, and maximum number of packets per second. For example, in Figure 5–48, the maximum number of packets per second during this capture session was 87, while the maximum percentage of bandwidth utilization was five percent.

Run Information

The Run Information counters provide statistics about the current capture session as follows:

Bandwidth

The theoretical maximum amount of traffic that could travel over the network being analyzed. For example, the Bandwidth counter for Ethernet is 10 Mbps. For networks that do not have an established theoretical maximum (such as WANs) the analyzer can use a variety of algorithms to "figure out" the theoretical maximum.

Duration

The length of time between the first frame accepted into the analyzer's capture buffer during the current capture session and the most recent frame accepted into the capture buffer. The Duration counter is incremented each time a new frame is analyzed by Expert. The increment is based on the elapsed time between the accepted frame and the previous frame.

The Elapsed time counter (in the upper-right corner of the display) simply keeps a running total of the time elapsed since capture was started. Whereas the Elapsed time counter has an upper limit of 99:59:99 (100 hours), the Duration counter will measure accurately up to a maximum period of 42 days.

There will sometimes be some discrepancy between the Duration counter and the Elapsed time counter in the upper right corner of the display. This can happen for the following reasons:

- When capture is paused, the Elapsed time counter does not increment. However, the Duration counter is measuring real time since the first frame was accepted. Therefore, when capture is resumed, the Duration counter will jump ahead to where it is higher than the Elapsed time counter. The amount of time the Duration counter is greater than the Elapsed time counter will be equal to the amount of time capture was paused.

- Under heavy traffic loads, the clock may be slow as the analyzer devotes more processing time to incoming traffic. As the analyzer catches up, the clock will be updated.

Start run

The time and date the current capture session was begun.

The time and date correspond to those that the PC regards as current. If the PC's time and date are incorrect, the analyzer's will be as well. You can use the DOS commands `Time` and `Date` to change the time and date the PC regards as current.

% Analyzed

Because the amount of data passing over a network segment is potentially huge, the Expert analyzer will sometimes develop a backlog of frames waiting to be analyzed. The % **Analyzed** counter details how much of the data from the current capture session has been analyzed. During heavy traffic loads, this counter may fall below 100 percent. When capture stops, the analyzer will continue to perform Expert analysis until all unanalyzed frames still in the capture buffer have been processed.

NOTE: Under heavy traffic loads, the Expert will sometimes skip frames, never performing Expert analysis on them. At the end of a capture session, the % **Analyzed** counter indicates the percentage of total frames (that is, those seen during the current capture session) analyzed, giving you an idea of how many frames the Sniffer "saw" but was unable to analyze.

Effects of Capture Filters on Global Statistics

The statistics in the Global Symptoms window are based solely on those frames that reach the capture buffer. If you have set capture filters (such as protocol filters, station address filters, or destination class filters), various frames that do not pass these filters will never reach the capture buffer. Accordingly, the Expert analyzer's Global Statistics will not take these frames into account. This can render the Expert's statistics inaccurate.

This is particularly misleading in the case of the capture filters for protocols. For example, if in a DECnet environment you set a capture filter to exclude all DRP frames, the Expert analyzer will falsely report that a very small percentage of your network traffic is DECnet. To ensure accurate statistics, set capture filters carefully.

Effects of Frame Size Option on Global Statistics

The **Frame Size** option allows you to specify (in bytes) what portion of each frame is passed into the capture buffer by the Expert analyzer. You can boost capture performance by "slicing" frames after 32, 64, 128, 256, and 512 bytes. However, because the Expert analyzer bases its Global Statistics solely on data into the capture

buffer, frame slicing can cause inaccurate statistics in the Global Statistics window. On token ring networks with network utilization greater than 50%, set the frame size option to 256 bytes.

NOTE: The Expert analyzer needs the first 256 bytes of each frame to compile accurate Protocol Family statistics. If **Frame Size** is set lower than 256 bytes, inaccurate Protocol Family statistics will result.

Advanced Navigation Techniques

This section describes several advanced techniques for navigating through the Expert window. As you grow more comfortable working with the Expert analyzer, these techniques will speed your work with the analyzer. They include:

- **Higher layer/Lower layer** function keys
- **Next symptom/Previous symptom** function keys

Using the Higher Layer/Lower Layer Function Keys

During post-capture display (or, while capture is paused), several function keys let you trace the displays relating to a specific network object through the four Expert layers without having to return to the Expert Overview. For example, you could use the **Lower layer** key to trace the displays relating to a particular application from the Application layer down to the DLC Station layer. This eliminates the need to return to the Expert Overview before investigating related displays at another layer.

The **Higher layer/Lower layer** function keys are not available while the analyzer is actively capturing frames. You can only use them while capture is paused or during post-capture display. Also, for some protocols, the **Higher layer/Lower layer** function keys may not be available.

To use the Higher layer/Lower layer function keys:

1. In a Summary, Detail, or Statistics window at any of the four Expert layers, use the cursor keys to highlight the application, connection, network station, or DLC station of interest.
2. If the analyzer is capturing frames, pause capture by pressing F9.
   Result: Additional key labels appear for F7 **[Lower layer]** and F8 **[Higher layer]** (Figure 5–49).

NOTE: If the highlighted object is at the Application layer, the key label for F8 **[Higher layer]** will not appear, because there is no higher layer. Similarly, the key

label for F7 **[Lower layer]** will not appear if the highlighted object is at the DLC Station layer because there is no lower layer.

F7 (Lower layer) label appears when capture is paused or during post-capture display.

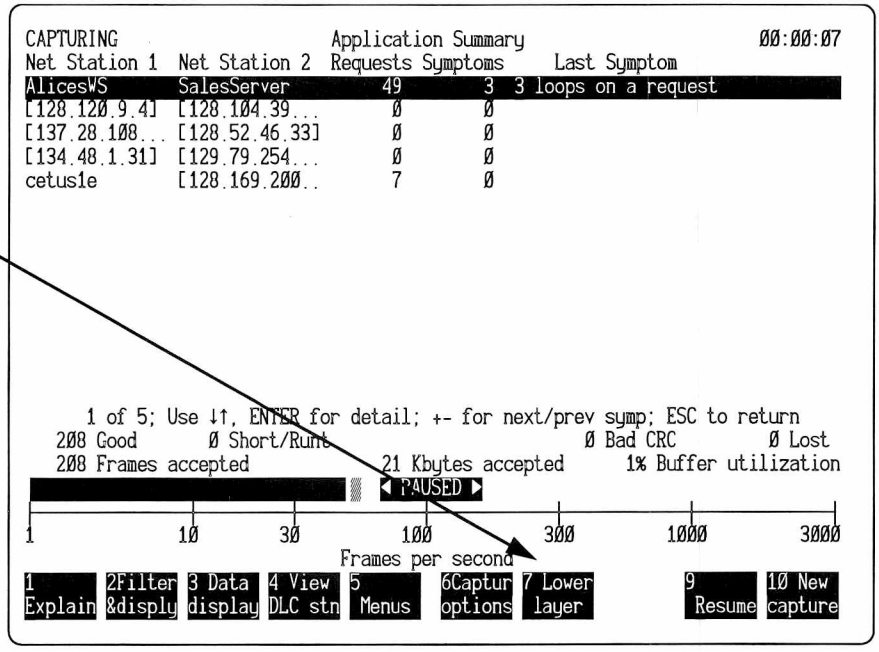


Figure 5–49. Application Summary screen with F7 (Lower layer) visible

3. Press F7 **[Lower layer]** or F8 **[Higher layer]**.

   Result: The object related to the highlighted object appears at the higher or lower layer, depending on which key was pressed. For example, if the highlight was on the application between the two stations **AlicesWS** and **SalesServer** (as in Figure 5–49) and F7 **[Lower layer]** was pressed, the display would now show the Connection Summary window with the corresponding connection highlighted (as in Figure 5–50).

NOTE: If you press F7 **[Lower layer]** from a Connection layer Summary or Detail window, the pop-up box in Figure 5–50 appears. Because there are two network stations associated with a connection, the analyzer prompts you to select which of the two related network stations you want to see highlighted in the Network Stations window.

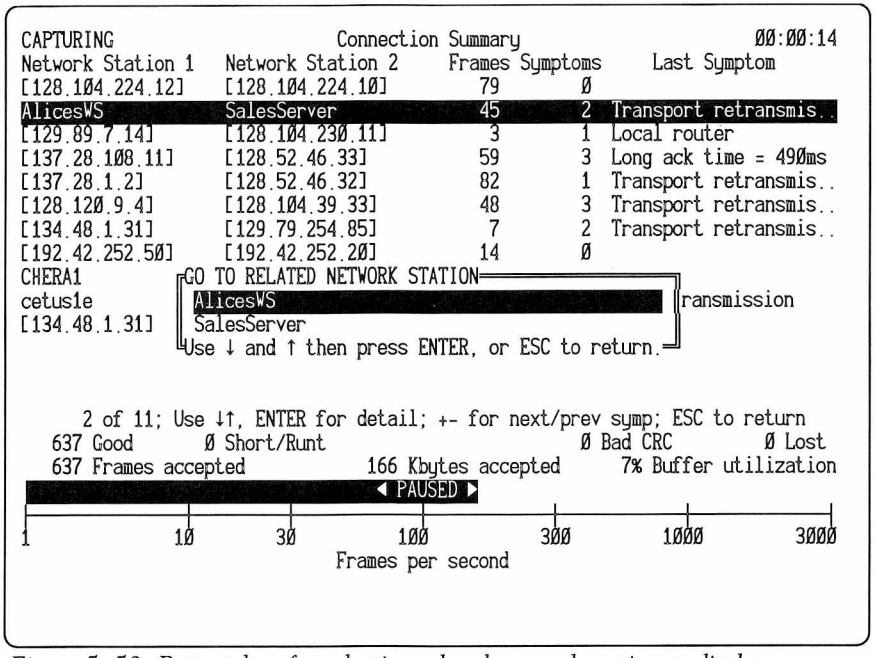


Figure 5–50. Pop-up box for selecting related network station to display

Using the Next Symptom/Previous Symptom Keys

You can also use the **+ (Next symptom)** and **- (Previous symptom)** keys to speed your navigation of the Expert window. These keys allow you to skip automatically between network objects that have symptoms associated with them. These keys are available in the displays accessible from the Objects/Symptoms column of the Expert Overview.

The **Next symptom/Previous symptom** keys are particularly valuable in the Detail and Statistics windows. You can use them to scroll automatically to the Detail or Statistics window for the previous or next network object with associated symptoms. This eliminates the need to return to the Summary view to find a network object with associated symptoms.

To use the Next symptom/Previous symptom keys:

1. In any display accessible from the Objects/Symptoms column of the Expert Overview, press **+ [Next symptom]** or **- [Previous symptom]**.

   The display for the next or previous (depending on which key was pressed) object which has associated symptoms appears. The display corresponds to the display from which F2/F3 was pressed. Detail windows will appear from Detail windows, Statistics windows will appear from Statistics windows, and so on.

If there are no previous symptoms and **- [Previous symptom]** is pressed, nothing happens. Similarly, if there are no later symptoms and **+ [Next symptom]** is pressed, nothing happens.

Function Keys in the Expert Window

This section describes the various function keys available in the Expert window. Different Expert displays have different associated function keys.

During Capture:

+/-	The plus and minus keys allow you to move display to the next or previous symptom respectively.
F2	From the Expert Overview, pressing the F2 key displays the Global Statistics window.
F4	In the Summary displays, the F4 key allows you to change the format of the current Expert window. The available formats for the Summary window are described on page 5–43.
F7/F8	In the Diagnosis Summary and Diagnosis Detail windows, the F7 and F8 keys allow you to temporarily remove and restore diagnoses from the display. See page 5–12 for more information.
F9	F9 pauses capture temporarily. While capture is paused, the following additional function keys become available:
F10	F10 stops capture and returns you to the Main Menu of the analyzer.

While Capture is Paused

+/-	The plus and minus keys allow you to move display to the next or previous symptom respectively.
F1	F1 provides a context-sensitive Explain message, displaying important information about the highlighted symptom or diagnosis.
F2	In the Expert Overview, pressing the F2 key displays the Global Statistics window. In a Summary or Detail display, the F2 key acts as a toggle for setting and removing **Network object** filters.

	For more information on **Network object** display filters, see the sections beginning on page 7–17.
F3	F3 toggles between the analyzer's Expert and Classic display windows.
F5	F5 takes you to the analyzer's main menu.
F6	F6 provides a menu of Capture-related options.
F7/F8	In the Diagnosis Summary and Diagnosis Detail windows, the F7 and F8 keys allow you to temporarily remove and restore diagnoses from the display. See page 5–12 for more information. In displays accessible from the Objects/Symptoms column of the Expert Overview, F7 moves display to the next lower layer associated with the highlighted object, while F8 moves to the next higher layer associated with the highlighted object.
F9	F9 resumes a paused capture.
F10	F10 starts a new capture.

Capturing Frames

6

Capturing Frames

Overview

This chapter describes capturing frames in Classic mode (as opposed to Expert mode, which was described in the previous two chapters) During Classic capture, the Sniffer analyzer passes those frames that pass its capture filters to the capture buffer. As frames are captured, the analyzer displays the results of the capture process in displays that are updated continuously. These displays show either a skyline view that shows traffic density over time, or tables that show station addresses. For ARCNET and LocalTalk, there is also a display that shows a Matrix view.

Before you start capture, you can customize the process to make sure the frames that interest you are captured. To do this, you can prepare for capture by defining various associated options that determine *how* frames will be captured, *which* frames will be captured, and how the capture will be *stopped.*

In addition to describing the **Cable test** feature for Ethernet networks, this chapter describes the options related to capturing frames. This includes:

- Preparing to capture frames
  - Displaying information about the capture buffer
  - Choosing a capture mode
  - Defining capture options
  - Defining capture filters
  - Defining a trigger to stop capture
- Starting the capture
- Options after you stop capture

When capture is complete, the captured frames are interpreted by the protocol interpreters, which interpret and decode the higher-level protocols within the frames. You can then examine the frame-by-frame results in various displays. These topics are discussed in Chapter 7, "Displaying Interpreted Frames."

Capture Menu Overview

Figure 6–1 provides an overview of the basic menu items associated with the Capture menu. Many of these items, in turn, are associated with additional options. Although

Figure 6–1 shows the menu as it appears on an Ethernet Sniffer analyzer, the basic Capture menu items are similar for all networks.

As with all other menu options, you first press the Cursor keys to move the highlight to the desired option. You can then define that option.

- For options marked with the √ and x symbols, you can press Spacebar to enable (√) or disable (x) the option. To reverse all settings, press CTRL-Spacebar.
- For options connected with a vertical bar (radio control), you can choose one of those options by moving to it and pressing Spacebar.
- For options where you must define a specific value, such as an address, you can choose a value from a list or enter the desired value into a dialog box.

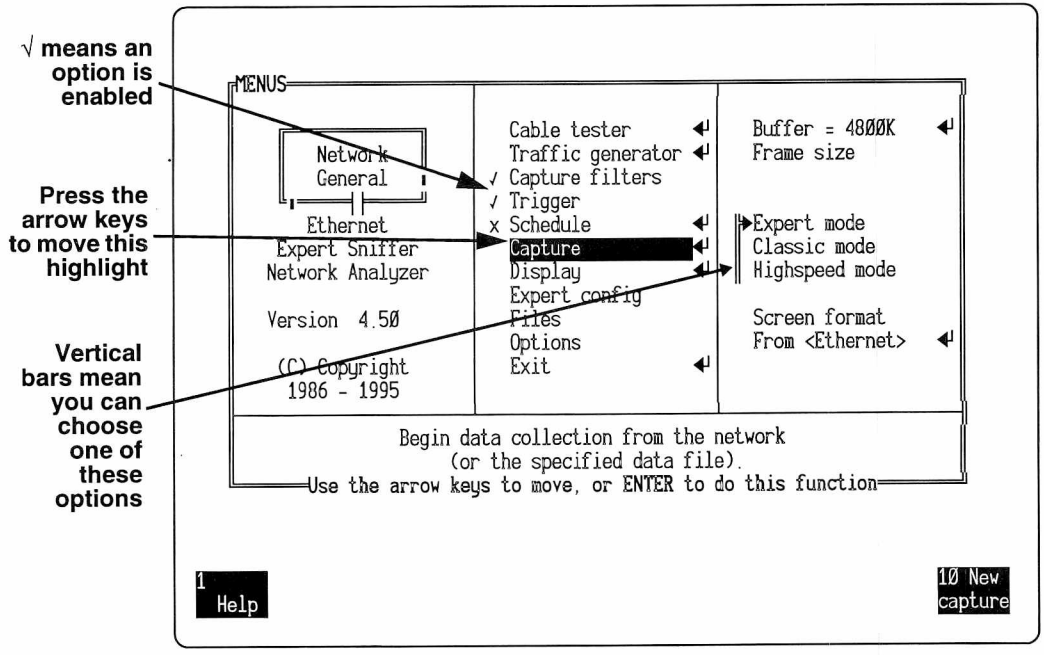


Figure 6–1. Overview of the Capture menu options

Ethernet Cable Tester

On Ethernet, the Sniffer analyzer provides a cable tester: a means to check and report cable faults. The analyzer's main menu includes an option labeled **Cable tester** (Figure 6–1). The cable test uses the analyzer's interface card as a time-domain reflectometer. During the test, the analyzer repeatedly emits a pulse and listens for the echo characteristic of certain types of faults.

NOTE: The Cable tester is not available on the Notebook Sniffer Analyzer.

To test the Ethernet segment for cable faults:

1. In the analyzer's main menu, move the highlight to **Cable Tester** and press ENTER (Figure 6–1).

   Result: The analyzer repeatedly emits a test signal on the Ethernet segment to which the network analyzer's interface card is attached. The analyzer overlays a display reporting what faults—if any—have been detected, and updates it as the test is repeated.

2. To terminate the test, press ESC.

The cable tester keeps testing until you terminate it by pressing ESC. While the test is running, the analyzer does not perform any of its other functions.

As long as the tester is active, the Sniffer analyzer repeatedly updates the display so that it shows the cable's current status. As long as it detects no fault, it displays the message `No cable fault found`.

The analyzer can detect a cable fault located between the adapter card and the transceiver that connects it to the network. It can also detect an open line or a short in the network cabling beyond the transceiver. The Sniffer analyzer cannot test for faults, open lines, or shorts on cable segments separated by a bridge or repeater from the segment on which it is located.

Automatic Test at First Capture

Under some circumstances, when you start capture, the analyzer first runs a brief cable test. It does this automatically, without being asked. It runs the automatic test only when this is the first live capture since the analyzer program started.

If the automatic test discovers no fault, there is no display and the analyzer proceeds directly with capture.

If the automatic test detects a cable fault, the analyzer reports it, and gives you the choice to proceed with capture or to halt.

The automatic test sends a packet out onto the Ethernet cable. If you do not want this test run, you can disable it with the **Cable test** option in the analyzer's Options menu. For more information on this option, see Chapter 3, "Defining System Options and Scheduled Events."

Messages Provided by the Cable Tester

The Cable Tester will generate the following messages:

Cable OK	Means the cable is OK.

Cable short	Means there is a short somewhere on the cable.
Cable open	Means the cable is not terminated on at least one end.

In addition, the analyzer may generate the "Cable fault," or "Cable unknown fault," messages. This usually means that one of the following conditions exists:

1. The transceiver is not connected to the AUI port.
2. There isn't a BNC cable or valid LAN connection to the transceiver.
3. The BNC cable is open at both ends (no terminators).

Limitations of the Cable Tester

- The Sniffer analyzer readily detects an open line and produces a steady diagnostic display. The reflection characteristic of a short circuit between the center conductor and ground is harder to discriminate from a normal signal, so the analyzer sometimes misses it.
- Certain intermittent defects can produce a jittering display. As it continuously updates the display, the Sniffer analyzer may assign different diagnoses to a continuously changing situation.
- When a collision anywhere on the network coincides with a test pulse, the resulting signal is similar to the pattern produced by an open line. However, a collision produces no more than a momentary flicker.
- Transceivers vary in the way they transmit the test pulse and its echo. This variation in turn produces variation in the behavior of the cable tester. Most transceivers produce useful results, but some do not.
- Under heavy traffic loads, the cable tester will occasionally report "Cable open," when it is actually not. This is because the analyzer needs enough "room" on the wire to send out its test pulse. As traffic subsides, the display will change to read, "Cable OK."
- The frame used by the network adapter may disturb certain types of network interactions. The cable tester repeats the test continuously, and thus reduces network throughput. It is recommended that the cable test be used only for short periods of time.

Displaying Information About the Capture Buffer

Before you start a capture, you may want to display information about the size of the capture buffer and detailed memory statistics that include memory allocation for the capture buffer.

The Capture menu shows the number of kilobytes the computer has allocated to the capture buffer. In Figure 6–1, for example, the buffer size is 5456 Kbytes.

To check the size of the capture buffer:

1. Move to **Capture** and look at the **Buffer=** item.

   Note the buffer size (in kilobytes). If the buffer makes use of expanded memory, the number of kilobytes is followed by the letters EXP.

You can also display other details about the Sniffer analyzer's memory usage.

To display a summary of memory statistics:

1. Move to **Capture\Buffer** and press ENTER.

   The Sniffer analyzer displays a summary of memory utilization statistics, including DOS data space, expanded memory, and various components of the system heap, as shown in Figure 6–2.

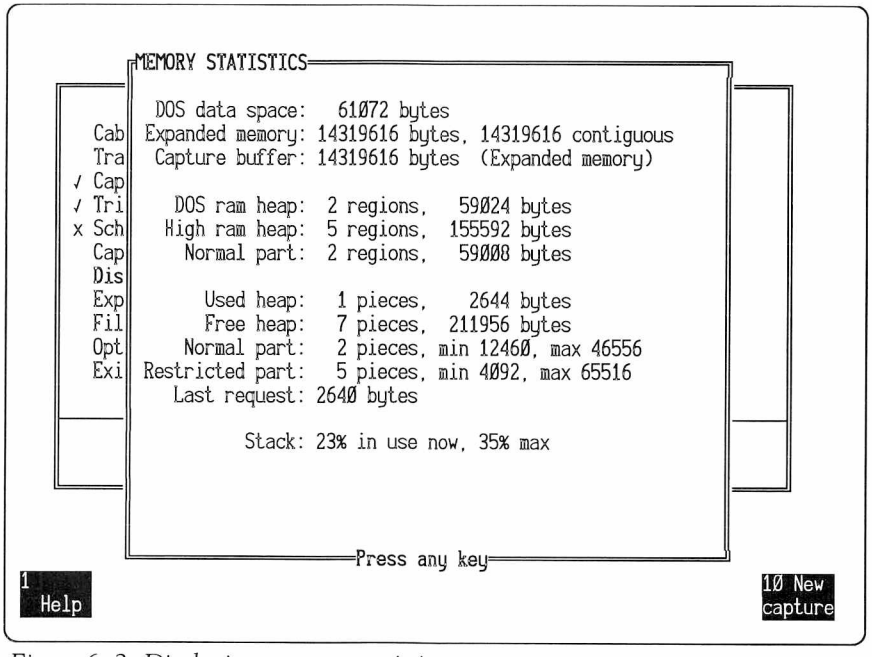

MEMORY STATISTICS
DOS data space: 61072 bytes
Expanded memory: 14319616 bytes, 14319616 contiguous
Capture buffer: 14319616 bytes (Expanded memory)
DOS ram heap: 2 regions, 59024 bytes
High ram heap: 5 regions, 155592 bytes
Normal part: 2 regions, 59008 bytes
Used heap: 1 pieces, 2644 bytes
Free heap: 7 pieces, 211956 bytes
Normal part: 2 pieces, min 12460, max 46556
Restricted part: 5 pieces, min 4092, max 65516
Last request: 2640 bytes
Stack: 23% in use now, 35% max
Press any key
1 Help
10 New capture

Figure 6–2. Displaying memory statistics

Preparing to Capture Frames: An Overview

Before you start to capture, you can specify how the system captures frames, which frames you want to capture, how to display information during the capture, and how to stop the capture.

In general, you should set these options before you start capturing. For each option, you can accept the predefined settings (defaults) or change them according to your needs. You can also save combinations of these options (setups) and apply these setups to later captures with the same criteria. For procedures for saving and loading a setup file, see "Saving the Current Options in the STARTUP File" on page 8–22. You can also disable most options temporarily or revert to the Sniffer analyzer's default options.

Figure 6–3 provides an overview of the tasks involved in preparing for capture. Not all options are listed in the table. Each task is described in more details in the sections that follow.

Preparing to Capture Frames

Choose a capture mode	Classic mode	
	Expert mode	
	Highspeed mode*	
Define capture options	Frame size	
	Capture source	Live network or data (trace) file
	Screen format	Units of measurement (frames or Kbytes)
		Tabular format (individual or pair counts)
		Skyline format (at defined intervals)
		Matrix format**
Define capture filters	Known/unknown stns	
	Destination class	
	Address match	
	Protocol	
	Pattern matches	
	Defective frames*	
Define stop of capture	Stop when full	
	Stop at trigger	Defective frames*
		External trigger
		Pattern trigger
		Trigger position (delay)
Define disk snapshot	Save at trigger or when full?	
	Size of snapshot files?	
	Number of files?	
	Overwrite files?	

*Ethernet, PC Network only
**ARCNET LocalTalk only

Figure 6–3. Preparing for capture: an overview

Choosing a Capture Mode

When your Sniffer Network Analyzer is shipped, it is set up to capture and display in **Expert mode**[1], with all options preset to reasonable default values. In addition to this mode, you can choose **Classic mode**. **Highspeed mode** is also available on PC Network or Ethernet analyzers to avoid losing frames during heavy traffic.

To choose a capture mode and the associated options:

1. Move to the desired option and press Spacebar.

   ▶ Expert mode (default)
   Classic mode
   Highspeed mode

2. Define the associated options, which are described in the sections that follow.

NOTE: The FDDI monitor is currently avail able with Classic mode capture only.

Defining the Basic Capture Options

In addition to defining the capture filters and the trigger that stops the capture, you can define the following basic options.

- The size of captured frames
- The capture source (live or from a file)
- The screen format of the views during capture

Defining Frame Size during Capture

You can choose to truncate frames that exceed a certain length to fit more frames into the capture buffer, thus extending the time covered by the capture and reducing the size of the capture data file and saving disk space (if you choose to save that file to disk). On a very busy network, truncation may also help avoid losing frames, since a longer frame takes slightly more time to store. The default is to capture the entire frame.

When each high-level frame is entirely contained within a lower-level frame, truncation leaves the headers and discards part of the high-level data. Since the headers usually contain the information you need for analysis, little is lost by discarding the later parts of the frame.

1. The FDDI Analyzer does not support the Expert or Highspeed modes.

However, some high-level protocols—such as TCP—are byte-oriented rather than frame-oriented, while others—such as ISO or X Window—permit very long messages. As a result, a single ISO or X message may span several lower-level TCP frames.

Figure 6–4 shows how a sequence of variable-length higher-level frames may be arbitrarily sliced and packed into frames of an intermediate byte-oriented protocol such as TCP. The start of a new spanned frame is not required to force a new lower-level frame. Thus, an X header (for example) may occur at any position in a TCP frame's data field.

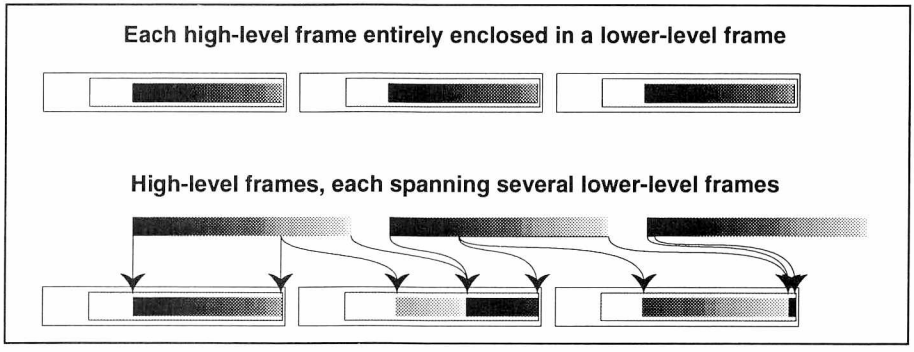

Each high-level frame entirely enclosed in a lower-level frame
High-level frames, each spanning several lower-level frames

Figure 6–4. Effect of high-level frames spanning multiple DLC frames

If your analysis requires keeping track of the headers of high-level spanned frames, it is *essential* to save whole frames. Otherwise, the headers and boundaries of the highest levels may be lost.

Defining the Capture Source: Live Network or Data File

You can determine whether data is captured from a live network or played back from a file. The capture option labeled **From <xxx>** determines the capture source. The default is to capture from the network, as indicated by the **<From Ethernet>**, **<From Token Ring>**, **<From FDDI>**, or **<From Synchronous>** items, as appropriate. After you set up a capture from a file, **From** is followed by the name of that file.

To capture from a file:

1. Move to **Capture\From <xxx>** and press ENTER. (**From** is at the bottom of the menu; if necessary, scroll down to display it.)

   A dialog box appears that shows the files that contain saved frames (trace files) in the CAPTURE directory of the analyzer's hard drive (Figure 6–5).

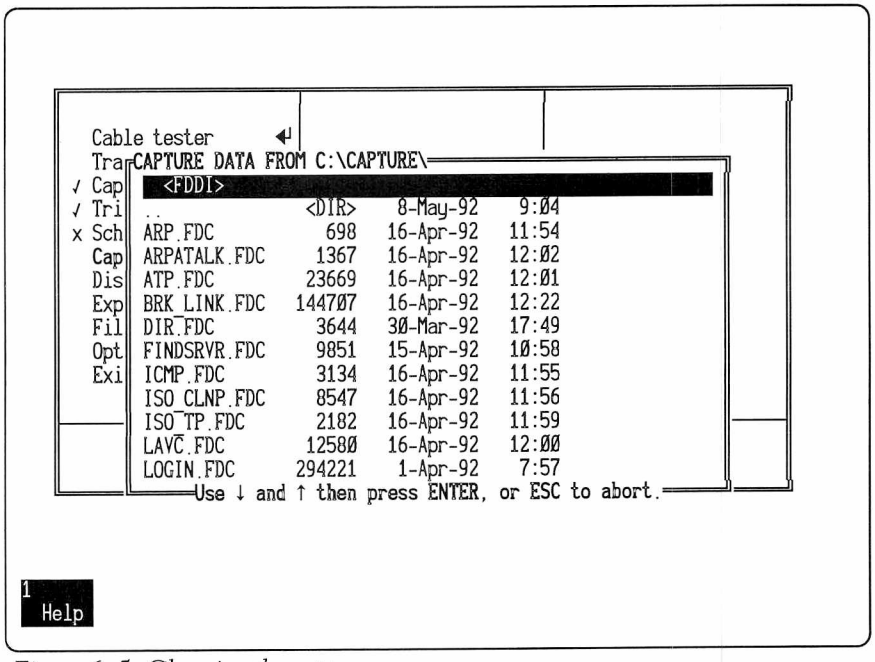


Figure 6–5. Choosing the capture source

2. Move to the file from which you want to capture and press ENTER.

   Note that the name of the selected file now appears after **From < xxx>**. The Sniffer analyzer reads this file into the adapter card and then sends the file to the capture buffer. All filters and the trigger are applied as the file contents are captured.

3. To move to a subdirectory other than the CAPTURE directory, move to **<DIR>**, press ENTER, and then select the desired directory.

Limitations of Capturing from a Saved Trace File

When you capture frames from a trace file, the analyzer cannot emulate the speed at which frames were captured from the network due to limitations enforced by the time required to access the disk drive (where the trace file is stored). Depending on your platform, capturing from a trace file is at least 20 times slower than the real captured traffic. That is, statistics relating to traffic rates will be at least 20 times slower during playback than they were during actual capture.

To capture from the network:

When the currently selected capture source is a file, you must reselect the appropriate network if you want to capture from the network.

1. Move to **Capture\From <xxx>** and press ENTER.
2. In the dialog box that appears, move to the network name (at the top of the screen) and press ENTER.

Defining Screen Format During Capture: An Overview

You can observe the capture process in different formats, depending on whether you are working with a LAN or a WAN/Synchronous network and on the **Screen format** options you define.

Screen Formats for LANs During Capture

For LANs, you can choose between various screen format options to display data as it is captured, including:

- Tabular views (called **Counts**), as either individual or pair counts
- Skyline view, at one of three intervals between updates
- Matrix view (ARCNET and LocalTalk only), which shows the running totals by source, arranged without labels in a 16x16 matrix.

For all views, you can define the count units used (frame counts, Kbyte counts, or network usage) and the scale of the bar graph that shows real-time traffic density (linear or logarithmic).

Figure 6–6 summarizes the LAN **Screen format** options for most LANs.

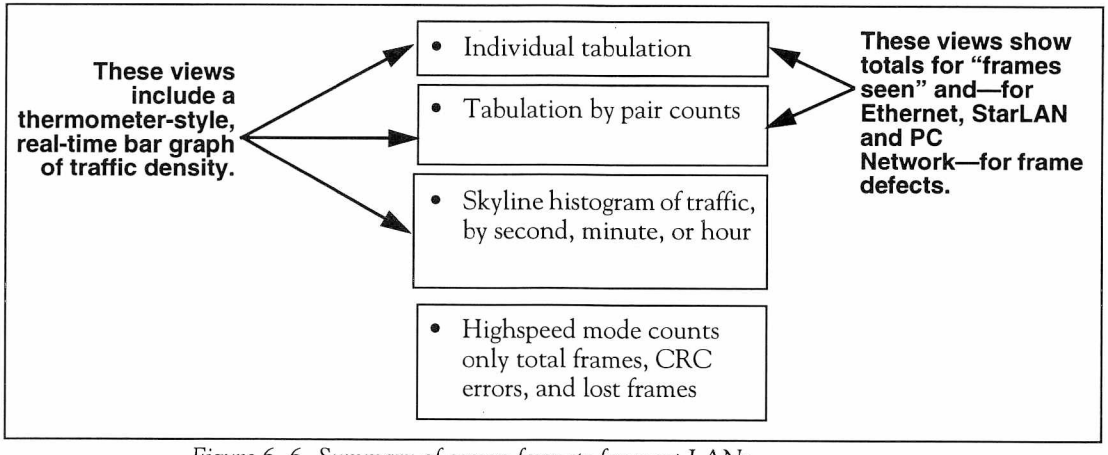

These views include a thermometer-style, real-time bar graph of traffic density.
• Individual tabulation
• Tabulation by pair counts
• Skyline histogram of traffic, by second, minute, or hour
• Highspeed mode counts only total frames, CRC errors, and lost frames
These views show totals for "frames seen" and—for Ethernet, StarLAN and PC Network—for frame defects.

Figure 6–6. Summary of screen formats for most LANs

Figure 6–7 illustrates these options.

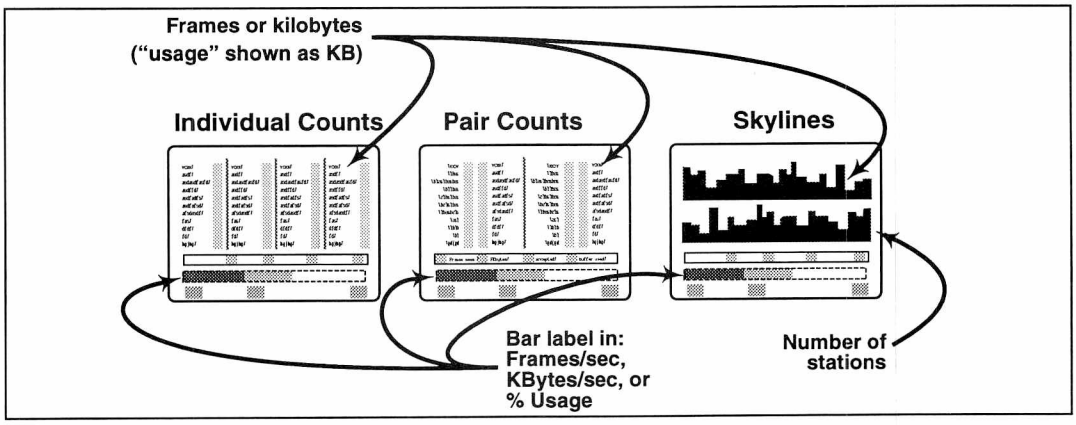


Figure 6–7. Effect of various screen format options

Screen Formats for WAN/Synchronous Networks During Capture

On the Sniffer Internetwork Analyzer, you can further define the following options associated with each of the screen formats:

- Tabular view: whether to display all stations or active stations only
- Skyline view: the interval between updates (the default)
- Both views: the units used to measure the capture (frame counts or Kbyte counts) and the scale of the bar graph that shows real-time traffic density (linear or logarithmic)

NOTE: Although the tabular view (**Counts**) is available when the **Router/Bridge** option is enabled, the screen will remain blank (except for the DTE/DCE counters and the various counters at the bottom of the screen). This is because the **Router/Bridge** option tells the analyzer to expect proprietary versions of HDLC. These versions do not conform to the traditional HDLC standard, and as such, traffic cannot be tallied according to the types of frames sent (such as Info, RR, RNR, REJ, and so on). When capturing with **Router/Bridge** enabled, it is best to leave the Skylines view (the default) enabled.

Defining the Screen Format During Capture: Procedure

Defining a screen format includes choosing between one of two tabular formats and the Skyline format. For all formats, you can define whether data is shown as frame counts, Kbyte counts, or in terms of network usage. You can also determine the scale of the bar graph at the bottom of the display.

Each option is explained in more detail after the procedure.

To select the screen format for most LANs:

1. Move to **Capture\Screen format** and choose desired units of measure.

   ▶Show frame counts (default)
   Show Kbyte counts
   Show NW usage

2. Choose the desired scale of the bar graph.

   Linear bar scale
   ▶Log bar scale (default)

3. Choose the desired display format.

   Individual counts
   ▶Pair counts (default)
   Skylines

   If you chose Skylines, define the interval at which the screen is updated.

   ▶1 second update (default)
   1 minute update
   1 hour update

To select the screen format for a WAN/Synchronous link:

1. Move to **Capture\Screen format** and choose desired units of measure.

   ▶Show frame counts (default)
   Show Kbyte counts

2. Choose the desired scale of the bar graph.

   Linear bar scale
   ▶Log bar scale (default)

3. Choose the desired display format.

   Counts
   ▶Skylines (default)

   If you chose Skylines, define the interval at which the screen is updated.

   ▶1 second update
   1 minute update (default)
   1 hour update

   If you chose Counts, define which stations are shown.

   Display all
   ▶Display active (default)

Units of Measure

You can select the units of measure in which capture activity is reported. The choices and their effects on individual counts, total counts, and the bar graph are shown in Figure 6–8. The default is to show frame counts.

Units of measure include:

- Frame counts

- Kilobytes
- Network usage (LAN only)

	Tabular units	**Skyline units**	**Bar graph units**	**Counters**
Frame counts	Frames	Frames	Frames	both
Kilobytes	Kilobytes	Kilobytes	Kilobytes	both
Network usage (LAN)	Kilobytes	Kilobytes	Percentage of bandwidth	both

Figure 6–8. Capture menu options for frames, kilobytes, and usage

Traffic Density Bar Graph

As capture proceeds, the Sniffer analyzer displays a thermometer-style horizontal bar graph that shows real-time variations in traffic density (Figure 6–9). If the **Audible clicks** option (Options menu) is enabled, the intensity of the clicks corresponds to the traffic density.

For LAN traffic, a single bar is updated several times a second. The bar shows a moving average of the last half-second's activity and the "high water" mark—the maximum activity recorded during the current capture session. Figure 6–9 shows a sample bar graph, with the Frames option enabled, for a LAN.

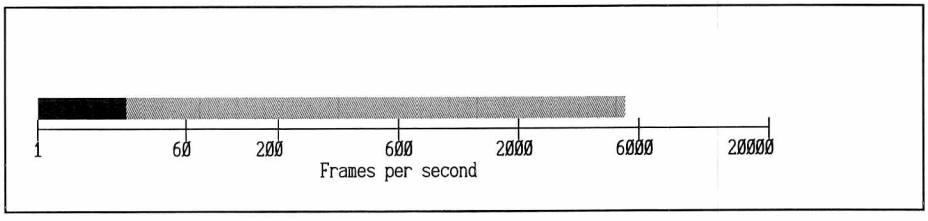


Figure 6–9. Traffic density bar graph for LANs (logarithmic scale)

For WAN/Synchronous traffic, there are two bar graphs; one for the DTE and one for the DCE counters, as shown in Figure 6–10.

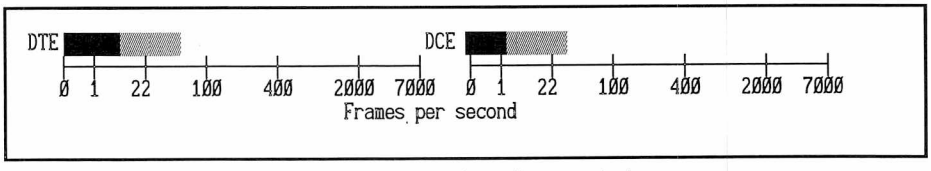


Figure 6–10. Traffic density bars for WAN/Synchronous link

You can select either a logarithmic or a linear horizontal scale for the traffic density bar graph.

Linear	A fixed distance (for example, 1 centimeter) corresponds to an absolute change in traffic density (for example, 10,000 frames).
Logarithmic	A fixed distance (for example, 1 centimeter) corresponds to a relative change (for example, 10 percent).

When the overall density is low, small variations are easier to see on a logarithmic scale (the default).

Information in the Tabular Views

In addition to the counters that provide information about frames and buffer utilization, the tabular displays show details about which stations are active. You can display this information as pair counts (transmitting and receiving stations) or as individual counts (transmitting stations only). Figure 6–11 shows a sample pair count display for Ethernet.

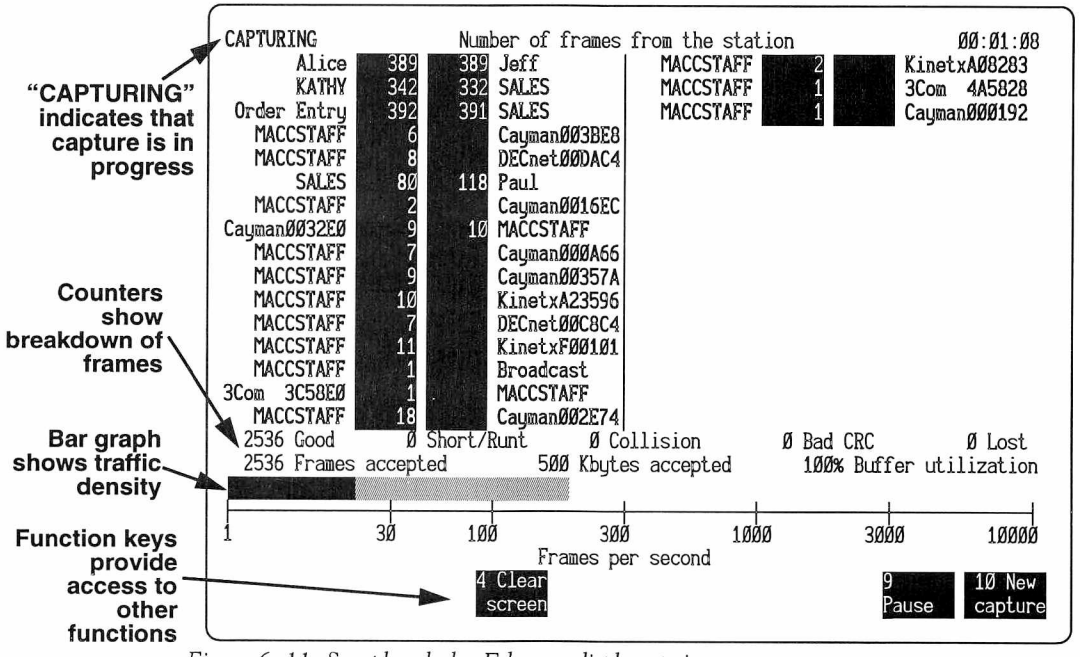

"CAPTURING" indicates that capture is in progress
Counters show breakdown of frames
Bar graph shows traffic density
Function keys provide access to other functions
CAPTURING
Number of frames from the station
00:01:08
Alice 389 389 Jeff
KATHY 342 332 SALES
Order Entry 392 391 SALES
MACCSTAFF 6 Cayman003BE8
MACCSTAFF 8 DECnet00DAC4
SALES 80 118 Paul
MACCSTAFF 2 Cayman0016EC
Cayman0032E0 9 10 MACCSTAFF
MACCSTAFF 7 Cayman000A66
MACCSTAFF 9 Cayman00357A
MACCSTAFF 10 KinetxA23596
MACCSTAFF 7 DECnet00C8C4
MACCSTAFF 11 KinetxF001101
MACCSTAFF 1 Broadcast
3Com 3C58E0 1 MACCSTAFF
MACCSTAFF 18 Cayman002E74
MACCSTAFF 2 KinetxA08283
MACCSTAFF 1 3Com 4A5828
MACCSTAFF 1 Cayman000192
2536 Good 0 Short/Runt 0 Collision 0 Bad CRC 0 Lost
2536 Frames accepted 500 Kbytes accepted 100% Buffer utilization
1 30 100 300 1000 3000 10000
Frames per second
4 Clear screen
9 Pause
10 New capture

Figure 6–11. Sample tabular Ethernet display: pair counts

Counters

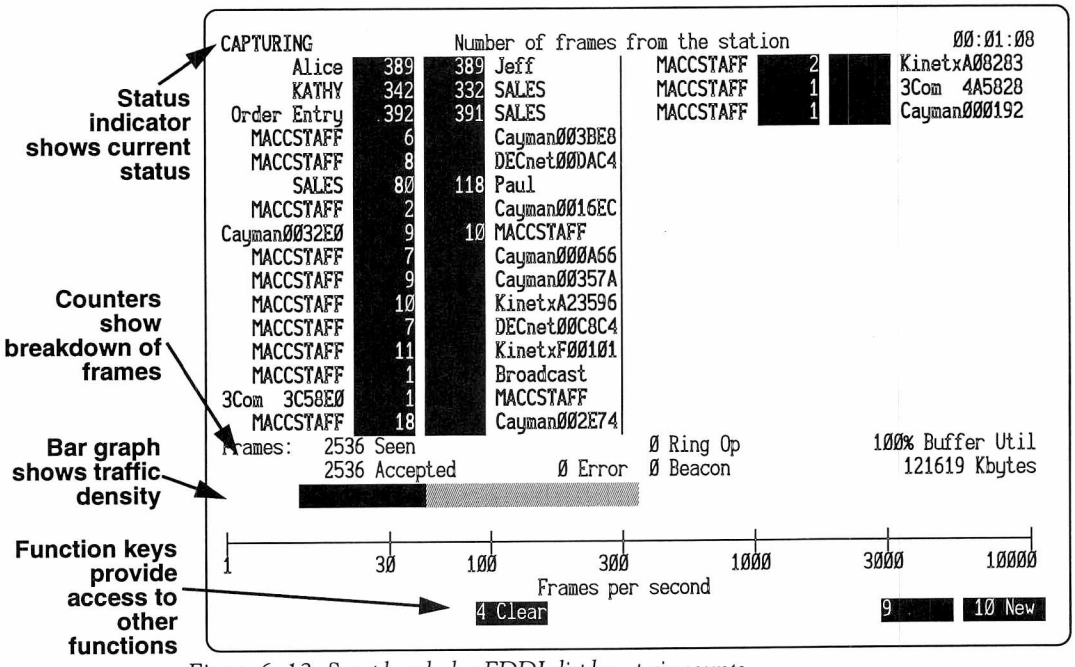


Figure 6–12. Sample tabular FDDI display: pair counts

As capture proceeds, you can see the total number of frames (whether or not they passed the capture filters) and the total number of kilobytes they contained. On token ring and FDDI networks, these totals are reported directly as "frames seen" and "kilobytes seen."

On other networks, there is no single total for "frames seen," but separate counts for various subtotals. On Ethernet, for example, there are totals for the total numbers of good frames, short/runt frames, bad CRC frames, and lost frames, as shown in Figure 6–11. On analyzers with Ethernet-II adapter cards, there is also a counter for collision frames.

On an FDDI analyzer, there are three counters whose function is not entirely self-evident — Error, Beacon, and RingOp.

- The Error counter is active only when capturing error frames. When the counter is active, the analyzer pre-scans all frames to derive the error count, regardless of how the other capture filters are set. The count includes frame fragments and all frames that have an invalid frame status field, a bad CRC, or the E-flag set.
- The Beacon counter applies to all frames regardless of how any of the capture filters are set. The analyzer pre-scans all the frames to derive the beacon frame count.

- The RingOp counter displays the RingOp value that is passed to the analyzer by the FDDI adapter. The count is updated once each second. This count indicates how many times the ring toggles from operational to non-operational status.

  When the analyzer is in beam splitter mode, the RingOp counter is also incremented when the analyzer's link is disconnected, even though there is no RingOp event on the ring being observed.

Buffer Utilization

During capture, the Sniffer analyzer continuously updates a counter that shows the percentage of the capture buffer that has been filled, up to 100 percent. When the buffer is full, the oldest frames are purged while capture continues.

Station Names

If the current name table includes the symbolic names associated with various DLC addresses, the analyzer displays those names in the tabular displays. These names make the displays more meaningful and make it easy to identify stations—and suspected intruders. If a symbolic name is not in this table, the analyzer displays only the DLC address.

On startup, the Sniffer analyzer loads the name table from the STARTUP.*xx*D file (where *xx* is a two-letter abbreviation for the analyzer's topology). To include symbolic names in the displays, you can edit this table to assign names to the addresses you expect to see during the capture. You can also capture for a while to detect unnamed addresses and then edit the table to include the corresponding names. For more information about making optimal use of the name table, see "Managing Names" on page 8–3.

Pair Counts During Capture: LAN

When displaying pair counts during capture, detected pairs fill the available screen positions until the screen is full (Figure 6–13). For each pair of stations, there is one counter for traffic in the direction first detected and another for traffic in the reverse direction, in either frames or kilobytes. The number closest to the station's name describes transmissions *from* that station *to* the other station.

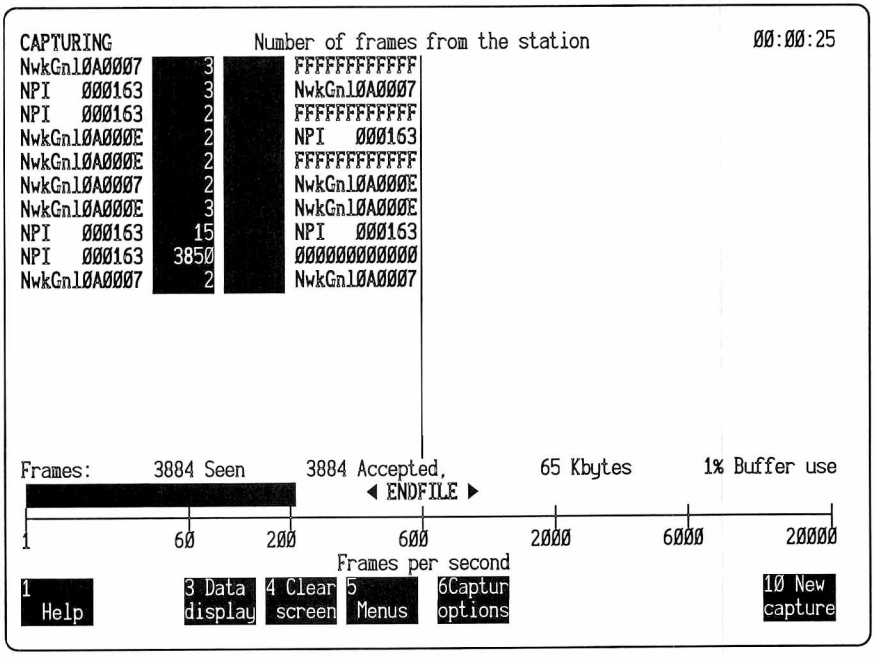


Figure 6–13. Sample tabular view: pair counts

When all available screen slots are filled, new pairs are not added to the screen. However, the counters that list the total and various subtotals continue to be updated. To clear the screen and start a new tabulation, press F4 **[Clear Screen]**.

NOTE: Clearing the screen has no effect on the frames in the capture buffer.

Individual Counts During Capture: LAN

As with pair counts, the Sniffer analyzer adds an entry for each station that transmits, in the order detected (Figure 6–14). Because these entries record the source but not the destination, there is more room for possible entries.

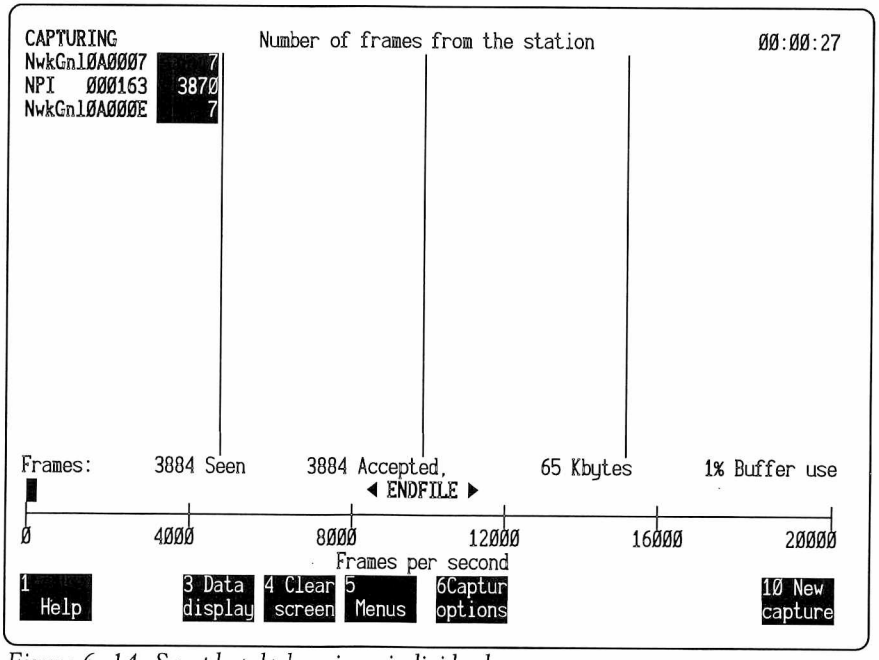


Figure 6–14. Sample tabular view: individual counts

When all slots on the screen are filled, grand total and detail counts are updated, although new stations that are detected are not listed. To clear the screen and start a new tabulation, press F4 **[Clear screen]**. Frames in the capture buffer are not affected.

Because ARCNET and LocalTalk use one-byte DLC addresses, there are exactly 256 possible addresses. For these networks, you can display individual counts in a matrix of 16 rows and 16 columns, labeled 0 through F. In the Matrix view, there is no room for symbolic names.

In the **Matrix** view on ARCNET networks, you can "probe" all stations, to find out which stations are on the network. Each station responds with one of the following replies, which appears at each station's slot in the display:

New	The station that responded to the probe did not appear in previous tallies.
Gone	The station appeared in previous tallies but did not respond to this probe.
n	A number indicates a station already known to be present. (0 indicates that no frames were transmitted, but the station responded to an earlier probe).

A dot serves as a place holder that represents an address that has neither transmitted nor responded to the probe.

To "probe" an ARCNET network:

1. With the Matrix view displayed, press F2 **[Probe network]**.

   In addition to the indicators that show new, gone, and current stations, the top of the screen shows the number of stations that responded since the last probe and whether or not they are still on the network. The totals below the columns show totals for the entire capture session.

Function Keys Available in the LAN Tabular Views

While observing a capture in one of the tabular views, the following function keys are available.

F2 (ARCNET only) **Network probe.** Pauses capture and "probes" all stations. Each station responds with "New," "Gone," "n," or "."

F4 **Clear screen.** Clears the screen and resets all counters to 0.

F9 **Pause.** Temporarily stops screen updates and displays a new set of function keys, listed as follows:

F1 **Help.** Displays the main Help menu.

F3 **Data display.** Interprets the frames in the capture buffer and displays them in the default (or chosen) display format.

F4 **Clear screen.** Clears the screen and resets all counters to 0. (This has no effect on the frames in the capture buffer.)

F5 **Menus.** Displays the main menu.

F6 **Capture options.** Displays the options for choosing the screen format.

F9 **Resume.** Resumes the display of the tabular views. If you changed any options, the views change accordingly.

F10 **Stop capture.** Stops the capture and redisplays the main menu.

Capture Screen Format: Special Counters for Token Ring

There are several counters in the capture screens that are unique to token ring. They are described below.

Counters and Timers for Token Ring-II

The counters above the bar graph in the capture screen have been enhanced for the Token Ring-II analyzer. These counters display the total number of frames seen by the analyzer during the capture period, the number of frames accepted into the buffer, the lost frames count, and the percentage of the buffer used. The ring speed (4 Mbps or 16 Mbps) is also displayed.

The lost frames counter does not give an exact count of the number of frames lost, but rather of the number of "lost frame" events. Each lost frame event corresponds to "one or more" lost frames. If the adapter becomes congested, the lost frame counter will be incremented each time the adapter reports a congestion error. This condition increments the counter by one, even though more than one frame may be lost. If frames are lost because the capture buffer is full, then the lost frames counter is incremented by one for each frame that is lost.

In addition to the counters, these indicators appear when the corresponding conditions exist on the ring:

- **Single Station** appears when the analyzer is the only station on the ring.
- **Ring Beaconing** appears when the analyzer is receiving or transmitting beacon frames.
- **Xmit Beacon** appears only when the analyzer is transmitting beacon frames.
- **Signal Loss** appears when the analyzer is receiving no signal from the ring.

Counters and Timers for Token Ring-III

The counters above the bar graph in the capture screen have been enhanced for the Token Ring-III analyzer. These counters display the total number of frames seen by the analyzer during the capture period, the number of frames accepted into the buffer, and the percentage of the buffer used. The ring speed (4 Mbps or 16 Mbps) is also displayed.

In addition to the counters, these indicators appear when the corresponding conditions exist on the ring:

- **Single Station** appears when the analyzer is the only station on the ring.
- **Ring Beaconing** appears when the analyzer is receiving or transmitting beacon frames.
- **Xmit Beacon** appears only when the analyzer is transmitting beacon frames.
- **Signal Loss** appears when the analyzer is receiving no signal from the ring.

Frame Counts Display During Capture: WAN/Synchronous

On a Sniffer Internetwork Analyzer, the tabular view shows counters for the X.25, HDLC, SNA, and Frame relay protocols, as well as a listing of detected calls. How

screens are displayed depends on how you defined the **Frame type** option when defining system options with the Options menu. For more information, see "Frame Type Options" on page 3–13.

As with the tabular views for a LAN, these views show various counters near the bottom of the screen, including CRC errors, lost frames, total frames seen, and the percentage of the buffer used. Also note that there are two bar graphs that show traffic density, one for DTE and another for DCE.

In addition, a one-line summary shows the status of the line, using the RS-232 indicators RxC, TxC, RxD, TxD, CTS, DSR, and DTR. The condition of each indicator is shown with an up arrow (for a logical 1), a down arrow (for a logical 0), and ↕, which means the indicator's status changed in the last second.

NOTE: Although the tabular view is available when the **Router/Bridge** option is enabled, the screen will remain blank (except for the DTE/DCE counters and the various counters at the bottom of the screen). This is because the **Router/Bridge** option tells the analyzer to expect proprietary versions of HDLC. These versions do not conform to the traditional HDLC standard, and as such, traffic cannot be tallied according to the types of frames sent (such as Info, RR, RNR, REJ, and so on). When capturing with **Router/Bridge** enabled, it is best to leave the Skylines view (the default) enabled.

NOTE: If you do capture in the tabular view with the **Router/Bridge** option enabled, the message, "`This screen intentionally left blank`" appears. The paragraph above explains why.

Figure 6–15 shows a capture using the **Frame relay** access protocol.

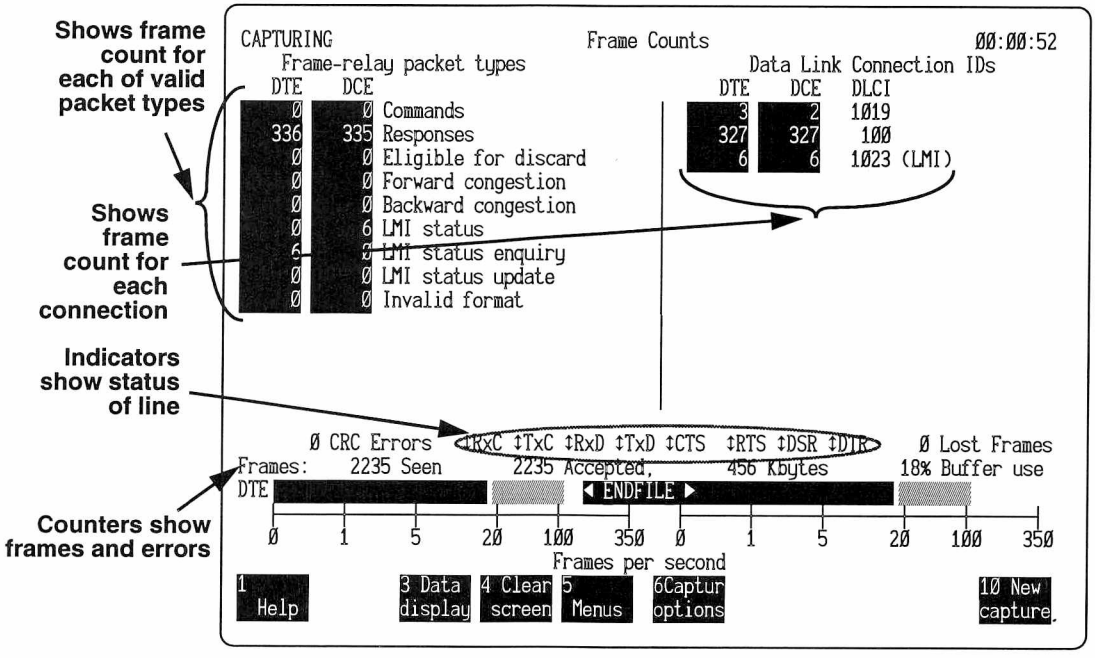


Figure 6–15. Internetwork Analyzer capture view: Frame relay access protocol

The left side of the screen shows the valid packet types supported by the Frame relay protocol, as well as the number of frame types detected during capture. The right side shows the number of connections during the capture. Each connection is identified by a unique number; the Data Link Connection ID (DLCI). Each DLCI can be assigned a particular type of connection—DLCI 1023, for example, is reserved for Frame Relay network management information (Local Management Interface).

Figure 6–16 shows a capture using the **X.25/HDLC** access protocol.

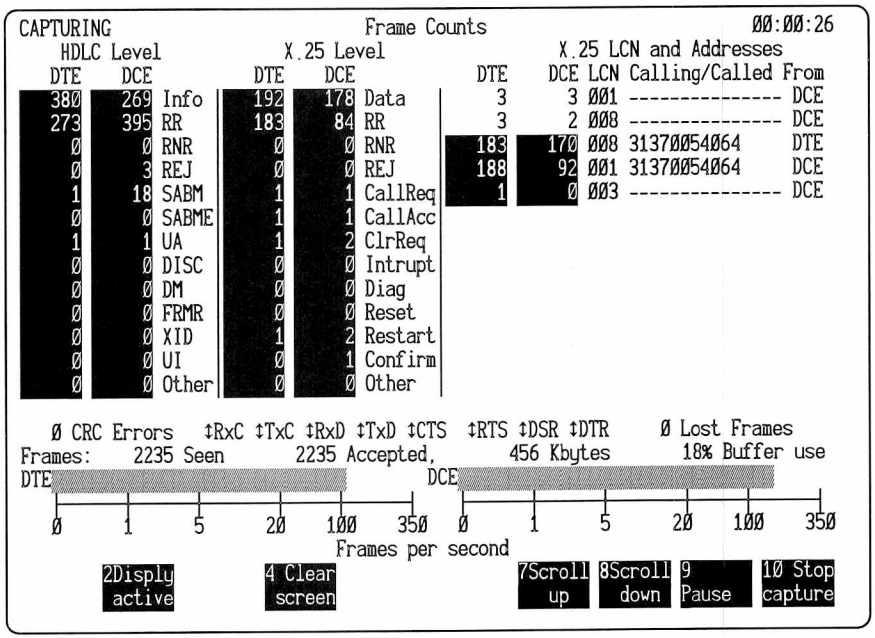


Figure 6–16. Internetwork Analyzer capture view: X.25/HDLC access protocol

The upper area of the screen consists of three main zones.

- The left zone shows the counters for each of twelve HDLC types, totaled separately by direction (from DTE and from DCE).
- The center zone shows the counters at the next protocol level, either X.25 or SNA. Because only data frames have SNA or X.25 content, the total number of frames in this panel may be lower than the total in the left panel.
- The right zone shows a table of logical calls, built in the order each call is detected within the traffic. Each call is identified by its call address (if known) and its logical call number (LCN), which is composed of a logical channel group number and the logical channel number. For calls that are not visible on the screen, you can use the Cursor keys or the function keys to scroll. The logical call table includes both calls that are still active and calls that have been completed. The counts for active calls are highlighted.

  A logical call's address is contained in the first frame. If a call was initiated before the Sniffer analyzer started to capture, its LCN is known, but the information is not in its address. Instead, this address is shown as a row of dashes, indicating an unknown address.

The column at the far right shows whether each call originated from DTE or from DCE. For each call, the analyzer tabulates traffic for that connection in each direction.

Active vs. Completed Calls

You can restrict the display to show only completed calls by pressing F2 **[Display active]**. Pressing F2 again restores the display to all calls. Once a call has been completed, its logical call number can be reused. As a result, inactive calls can include multiple instances of the same LCN.

Naming Addresses

As with LANs, you can supply names for the source or destination of a logical call. The analyzer substitutes the name for the remote address (the source on a call from DCE, the destination on a call from DTE). Names for addresses are visible in the right panel. For information about how to add names to the name table, refer to "Managing Names" on page 8–3.

Function Keys Available in the Sniffer Internetwork Analyzer Tabular Views

F2 **Display active/Display all.** Toggles the display between showing all stations or active stations.

F4 **Clear screen.** Clears the screen and resets all counters to 0.

F7 **Scroll up.** Scrolls the list of logical calls toward the top of the list.

F8 **Scroll down.** Scrolls the list of logical calls toward the bottom of the list.

F9 **Pause.** Temporarily stops screen updates and displays a new set of function keys that allow you to access the Help system, change the screen format, or interpret captured frames.

While paused, the following function keys are available:

F1 **Help.** Displays the main Help menu.

F2 **Display active/Display all.** Toggles the display between showing all stations or active stations.

F3 **Data display.** Interprets the frames in the capture buffer and displays them in the default (or chosen) display format.

F4 **Clear screen.** Clears the screen and resets all counters to 0. (This has no effect on the frames in the capture buffer.)

F5 **Menus.** Displays the main menu.

F6 **Capture options.** Displays the options for choosing the screen format.

F7 **Scroll up.** Scrolls the list of logical calls toward the top of the list.

F8 **Scroll down.** Scrolls the list of logical calls toward the bottom of the list.

F9 **Resume.** Resumes the display of the tabular views. If you changed any options, the views change accordingly.

F10 **Stop capture.** Stops the capture and redisplays the main menu.

Information in the Skyline View

The skyline view (Figure 6–17) shows traffic density during capture. Each view consists of two histograms, one above the other, with a common horizontal time scale. The top histogram shows the number of frames (or bytes) and the bottom shows the number of stations detected. You can manipulate the scale of each histogram to adjust the level of detail to the network's volume.

NOTE: If you are using a larger screen, the skyline views automatically expand to take advantage of the additional space. As a result, up to five histograms may be displayed.

Counters

The counters in the skyline view are the same as those in the tabular views. As capture proceeds, they show the total number of frames (whether or not they passed the capture filters) and the total number of kilobytes they contained. On token ring and FDDI networks, these totals are reported directly as "frames seen" and "kilobytes seen."

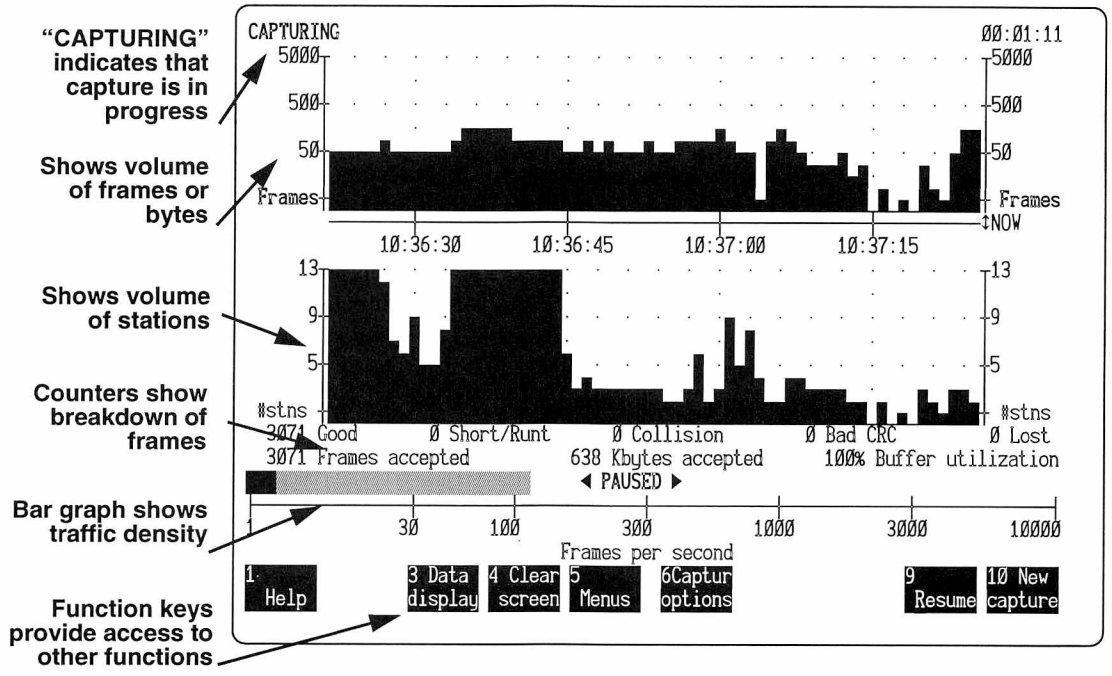


Figure 6–17. Sample LAN skyline view

On other networks, there is no single total for "frames seen," but separate counters for various subtotals. For example, on Ethernet, there are totals for the total numbers of good frames, short/runt frames, bad CRC frames, and lost frames. On networks with an Ethernet-II adapter card, there is also a counter for collision frames.

Buffer Utilization

During capture the Sniffer analyzer continuously updates a counter that shows the percentage of the capture buffer that has been filled.

Skyline Views for LAN Networks

On a LAN, the upper histogram shows either the number of frames or the number of kilobytes transmitted during the interval you specified, as shown in Figure 6–17. If you chose the **Show NW usage** option, the upper histogram shows the number of kilobytes and the bar graph shows the percentile of network usage. The lower histogram shows the number of stations active during the interval.

These histograms are updated with a new column at the right at the specified interval (1 second, 1 minute, or 1 hour). The Skyline view also provides a running count of total frames, but no itemization of traffic by individual stations.

Skyline Views for WAN/Synchronous Networks

On a WAN/Synchronous link (Figure 6–18), the upper histogram shows traffic from DTE, while the lower histogram shows traffic from DCE. Beneath the histograms are the counters that show the total number of frames (whether or not they passed the capture filters) and the total number of kilobytes they contained. In addition, there is a one-line summary that shows the status of the line, using the RS-232 indicators RxC, TxC, RxD, TxD, CTS, DSR, and DTR. The condition of each indicator is shown with an up arrow (for a logical 1), a down arrow (for a logical 0), and ↕, which means the indicator's status changed in the last second.

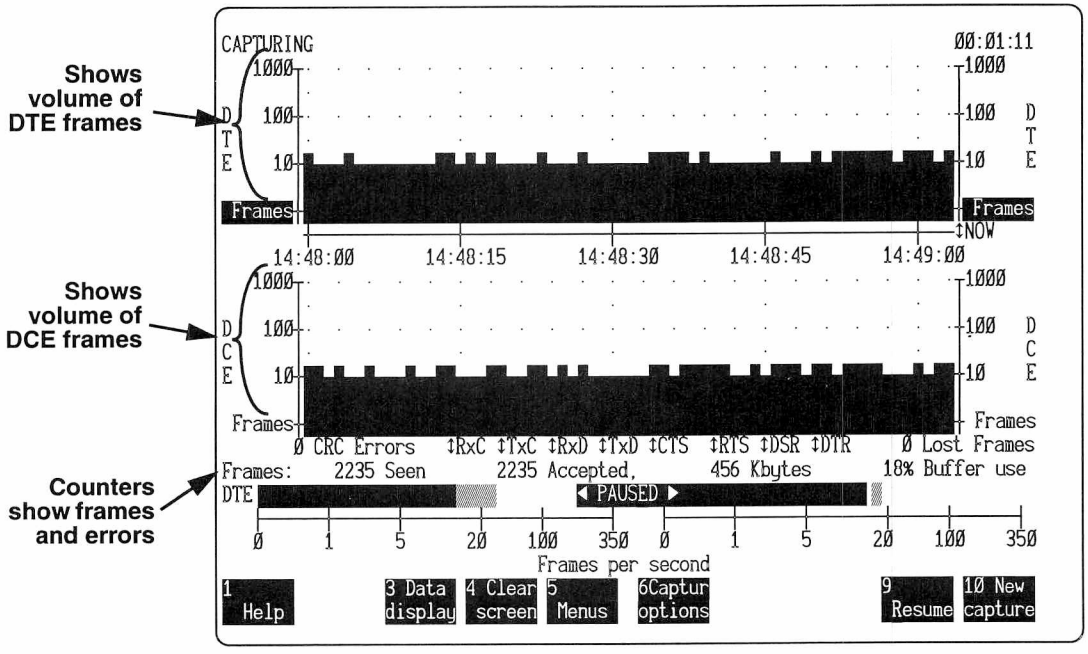


Figure 6–18. Sample WAN/Synchronous skyline view

Depending on traffic volume, you may want to manipulate the vertical scales of the two histograms to show the optimal level of detail. You can also manipulate the horizontal scale to show earlier intervals that are no longer in the view, as though backspacing through the display. You can adjust each histogram independently of the other.

To adjust the vertical scales to the best level of detail:

1. Press F2 **[Select display]** or the TAB key to select the histogram you want to scale.
2. To decrease the scale (larger bars related to a smaller range), press F6 **[Scale down]**.
3. To increase the scale (shorter bars related to a larger range), press F5 **[Scale up]**.

To adjust the horizontal scales to view earlier intervals:

1. Press F2 **[Select display]** or the TAB key to select the histogram you want to scale.
2. To view intervals that occurred earlier during the capture, press F7 **[View earlier]** repeatedly until you reach the desired interval.
3. After viewing earlier intervals, press F8 **[View later]** repeatedly until you reach any interval up to the current interval.

Function Keys Available in Skyline View

F2 **Select display** (or the TAB key)**.** Toggles between the two histograms.

F4 **Clear screen.** Clears the screen and resets all counters.

F5 **Scale up.** Increases the current histogram's scale to show a larger number of stations or frames. As the scale increases, the bars become shorter.

F6 **Scale down.** Decreases the current histogram's scale to show a smaller number of stations or frames. As the scale decreases, the bars become taller.

F7 **View earlier.** Allows you to view the number of stations, bytes, or frames at earlier intervals.

F8 **View later.** If you used function key F7 to view earlier intervals, this key returns you to later intervals, up to the current interval.

F9 **Pause.** Temporarily stops screen updates and displays a new set of function keys that allow you to access the Help system, change the screen format, or interpret captured frames.

While paused, the following function keys are available:

F1 **Help.** Displays the main Help menu.

F3 **Data display.** Interprets the frames in the capture buffer and displays them in the default (or chosen) display format.

F4 **Clear screen.** Clears the screen and resets all counters to 0.

F5 **Menus.** Stops capture and displays the main menu.

F6 **Capture options.** Displays the options for choosing the screen format.

F9 **Resume.** Resumes the skyline display. If you changed any options, the display changes accordingly.

F10 **Stop capture.** Stops the capture and redisplays the main menu.

Choosing Highspeed Capture Mode

When capturing "live" from Ethernet or PC Network, choosing **Highspeed mode** speeds up processing. During sustained high-speed traffic under certain conditions, the analyzer might not be able to capture every frame while simultaneously displaying it. Because the adapter card provides programmable access to the local buffer, you can store frames in the adapter card's temporary buffers instead of in the area of main storage dedicated to the Sniffer analyzer's capture buffer. Because the analyzer only counts frames instead of processing them, this speeds up the capture considerably.

Although the chosen screen format appears on the screen, it is not updated. Instead, a rectangle that shows the highspeed counts is superimposed on the center of the screen. As capture proceeds, only the central rectangle is updated, as shown in Figure 6–19. Note that the capture filters and the trigger options disappear from the menu when you choose **Highspeed mode**.

NOTE: If you are not using the Ethernet-II adapter card, storage is limited to the adapter card's buffer memory.

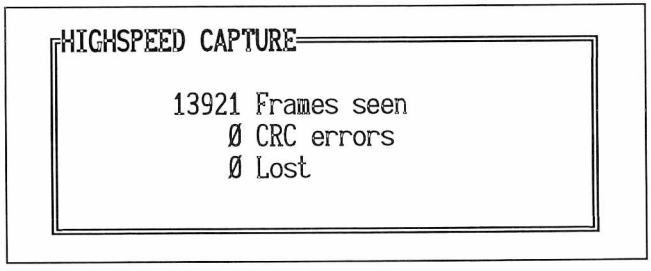


Figure 6–19. Information displayed during capture in Highspeed mode

If you are using an Ethernet-II adapter card, frames are transferred directly to the capture buffer as they are captured. Otherwise, pressing F10 **[Stop capture]** or F9

(**Pause**) transfers the accumulated frames in the adapter card's buffer to the Sniffer analyzer's capture buffer and displays the accumulated statistics.

To select Highspeed mode:

1. Move to **Capture \ Highspeed mode** and press Spacebar.

   Note that the **Capture filters** and **Trigger** options disappear from the menu. When you return to **Classic** mode, these options reappear, with the settings (enabled or disabled) intact.

Setting the Capture Filters

To limit the number of captured frames to those of interest, you can define filters that eliminate other frames, such as particular low-level DLC addresses or unknown stations. As a result, only those frames that pass the filters are captured. Which filters are available depends on your network.

Figure 6–20 shows the capture filters available for Sniffer analyzers with an Ethernet-II adapter card. The options associated with some of these filters will appear on the right when you move to a particular filter.

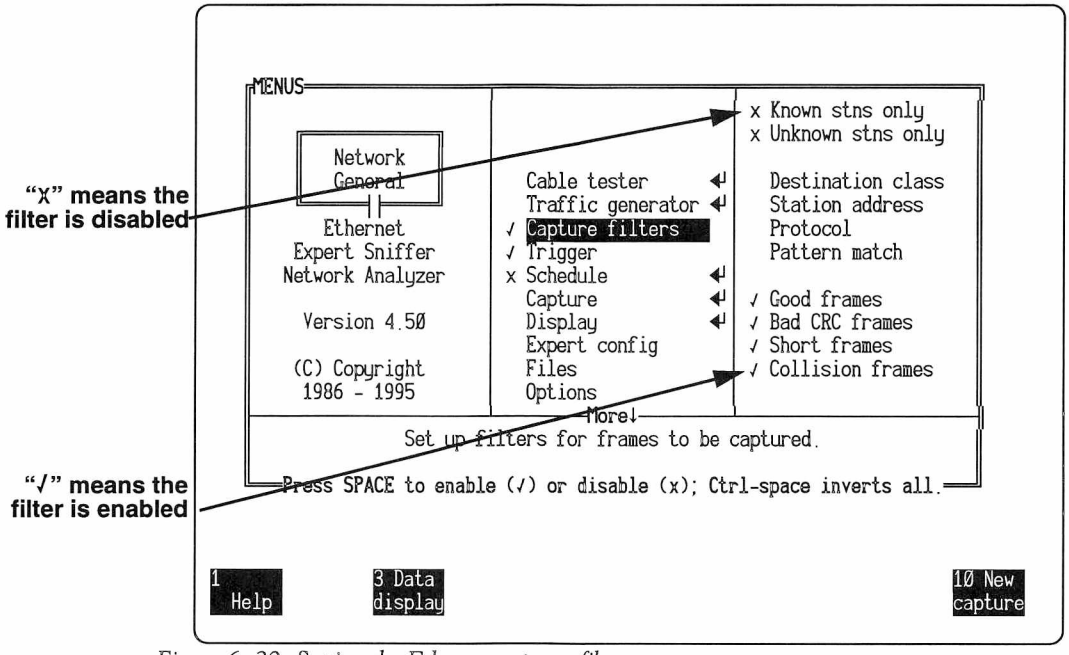


Figure 6–20. Setting the Ethernet capture filters

Figure 6–21 summarizes the available LAN capture filters by network.

LAN	Filter	Test	Default
All	Known stations only	Does a stations's DLC address have a corresponding symbolic name in the name table?	x don't accept
All	Unknown stations only	Does a station's DLC address *not* have a corresponding name in the name table?	x don't accept
All	Destination class	Does the frame have a specific destination or is it a broadcast/multicast?	accept both
All	Station address	Does the frame match any of the user-specified source-and-destination pairs?	accept any
All	Protocol	Does the frame contain any of the low-level protocols disabled by the user?	accept any
All	Pattern match	Does the frame match up to four user-specified patterns?	accept any
FD	Void/Claim frames	Is the frame a void or claim frame (for live capture only)?	x don't accept
FD	Error frames	Is the frame an error frame (for live capture only)?	x don't accept
EN*	Good frames	Does the frame contain frames without defects?	√ accept
EN*	Bad CRC frames	Does the frame include a C flag?	√ accept
EN*	Short frames	Is the frame less than 60 bytes long (runt)?	√ accept
EN-II	Collision frames	Does the frame include a collision?	√ accept

*Also for StarLAN and PC Network

Figure 6–21. Overview of available LAN capture filters

Figure 6–22 summarizes the available WAN/Synchronous capture filters.

WAN	Filter	Test	Default
	Pattern match	Does the frame match up to four user-specified patterns?	accept any
	From DTE	Does the frame include frames sent by the DTE?	accept any
	From DCE	Does the frame include frames sent by the DCE?	accept any
	RR frames	Does the frame include the RR (Receiver Ready) code?	accept any
	RNR frames	Does the frame include the RNR (Receiver not Ready) code?	accept any
	Info frames	Is the frame an SDLC/HDLC info frame?	accept any
	Good frames	Capture frames with good CRC?	accept any
	Bad CRC frames	Capture frames with bad CRC?	accept any

Figure 6–22. Overview of available Sniffer Internetwork Analyzer capture filters

Using capture filters requires a certain amount of processing time. As a result, the more complex the capture filter, the more time is required. On networks with a light or moderate load, this processing time is not noticeable. On heavily loaded networks, however, complex capture filters limit the speed at which the Sniffer analyzer can accept frames, unless the filters significantly reduce the number of frames accepted. As a result, some frames may be lost. If this happens, the number of lost frames is recorded in the *lost frames* counter. If the number of lost frames increases, try using simpler capture filters or (on Ethernet and PC Network) capture in **Highspeed mode**.

To set up the capture filters:

1. Move to **Capture filters**. If necessary, press Spacebar to enable (√) the option.
2. Move to the desired filters and press Spacebar to enable (√) or disable (x) those filters.
3. For filters with associated options, define those options.

Saving Selected Capture Filters

The capture filters you select remain in effect only until you exit the analyzer or reboot the computer. When shipped, the **Capture filters** option is enabled. To use the settings you defined instead of the system defaults, you can save them to a setup file and then load that file after you start the analyzer. You can also save them to the STARTUP.*xx*S file to be applied automatically.

NOTE: Saving a setup saves *all* options as you define them, not just the capture filters.

To save the capture filters setup:

1. Move to **Files \ Save \ Setups** and press ENTER.
2. In the dialog box that appears, enter the desired filename, without an extension.

Disabling the Capture Filters

If you observe a high number of lost frames, you may want to disable the capture filters or reduce their complexity. You may also find that the frames that interest you are not captured and suspect that a capture filter is eliminating those frames. By disabling the capture filters, you can determine whether the capture filters are responsible.

You can always disable filters individually or press CTRL-Spacebar to reverse all settings. There are also two general ways to disable any capture filters you may have enabled:

- Disable the **Capture filters** option.
- Use the **Use defaults** option.

By disabling the **Capture filters** option, you *temporarily* disable all capture filters. This allows you to see how capture proceeds with the filters disabled, without having to disable individual filters you may have spent considerable time setting up. After examining the results, you can fine-tune your capture filters.

To temporarily disable all selected capture filters:

1. Move to **Capture filters** and press Spacebar to disable (x) the option.

If you choose the **Use defaults** option, all enabled capture filters *and* all other options are reset to the default settings (shown in Appendix A). Because you may have spent considerable time defining various options, *do not* use the **Use defaults** option unless you want to return to the system defaults. This command is described in more detail in "Setting the Cable Test Option for Ethernet" on page 3–7.

Capture Filters and the Name Table

Several capture filters—**Known stations only**, **Unknown stations only**, and **Destination class**—use information contained in the name table. To use these filters efficiently, you must maintain this table.

The permanent name table is contained in the file STARTUP.*xx*D, which is read at system startup. This table includes any addresses that were previously detected and then named. In addition to this permanent name table, the Sniffer analyzer creates a current name table for each new capture by scanning the capture buffer for addresses that are not in the name table. If such addresses are found, the analyzer inserts them at the top of the name table. The working name table thus includes all the information in the permanent name table, as well as newly detected addresses (Figure 6–23).

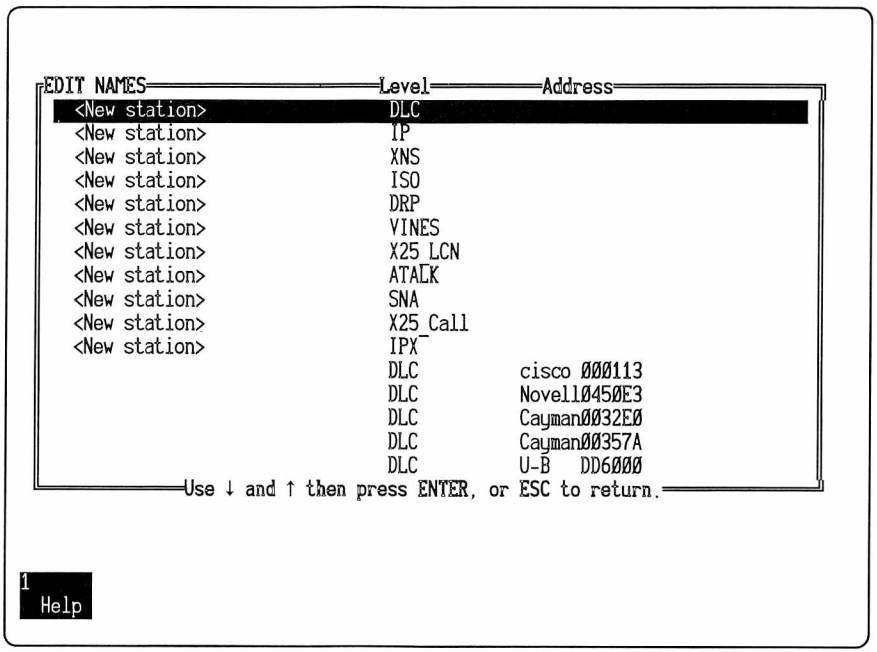


Figure 6–23. The working name table

Until you name the newly detected addresses, the Sniffer analyzer considers them "unknown." If the **Look for names** option is enabled (**Display\Manage names\Look for names**), the analyzer automatically updates the working name table with any detected addresses. Any unnamed addresses are deleted from the name table when you exit the Sniffer analyzer application. For additional information about working with the name table, refer to "Managing Names" on page 8–3.

Known Stations Only Filter

When you enable **Known stns only**, the analyzer captures only those frames that contain a "known," or named, DLC address (source or destination). To use this filter effectively, you must update your name table to name any detected addresses.

The default is x **Known stns only** disabled.

To restrict capture to frames from known stations:

1. Move to **Capture filters \ Known stns only**, and press Spacebar to enable the option (/).

Unknown Stations Only Filter (LAN)

When you enable **Unknown stns only**, the Sniffer analyzer captures only those frames that contain an "unknown" DLC address (source or destination). The analyzer considers an address to be unknown either when its address isn't in the current name table or when the address is not named.

The cause of such traffic could be illegal hackers, bad data frames, faulty software in the application or on the network, or adapter cards that were replaced without notifying the system manager.

The default is x **Unknown stns only** disabled.

To restrict capture to frames from unknown stations:

1. Move to **Capture filters \ Unknown stns only**, and press Spacebar to enable the option (/).

Destination Class Filter

On a LAN, you can specify whether to capture frames from a specific address, from a generic address, or from both. When you enable the **Broadcast** option, only frames transmitted to the generic address that includes several—or perhaps all—stations will be captured. When you enable only the **Specific** option, only frames transmitted to a specific address will be captured. Because there are no such transmissions over wide area networks, there is no **Destination class** filter for WAN/Synchronous links.

In the name table, you can assign a name to a generic address, such as "Error Monitor" or "LAN Manager." Of course, a generic address can only be the destination, not the source, of a frame. Each type of network has prescribed formats for generic addresses, which are different from any possible individual addresses.

Formats of generic addresses are summarized in Figure 6–24.

Originating Network	Type	Description	Characteristic Address
Ethernet StarLAN PC Network	Multicast address (including Broadcast)	A multicast address is a collective name for several stations. It may be a role played by one or more stations, or by all stations (for example, "Broadcast").	A DLC multicast address has a 1 in the low-order bit of the first byte, so that in hexadecimal its second character is odd (that is, 1, 3, 5, 7, 9, B, D, or F). No individual station has an address with that bit on.
Token Ring, FDDI	Functional address (including Broadcast)	A functional address is a collective name for a role played by one or more stations, (for example, "Error monitor") or by all stations (for example, "Broadcast").	A DLC functional address has a 1 in the high-order bit, so that in hexadecimal it appears as a number whose first digit is 8 or higher. No individual station has an address with that bit on.

Figure 6–24. Formats of generic addresses, by network of origin.

To select or exclude frames by destination class:

1. Note the meaning of broadcast or multicast address on your network.
2. Move to **Capture filters\Destination class** and press Spacebar to enable (√) or disable (x) the **Broadcast** and/or **Specific** options.

Station Address Filters

During capture, you can filter only for lower-level addresses. For these addresses, you can enable up to four different DLC address matches, where each match consists of the following information:

- The source and destination addresses
- Whether to include traffic that travels in both directions between those addresses
- Whether the filter includes or excludes this match

To make it easy to describe these matches, you can also assign a name to each match.

On a LAN, you can set filters for a frame's DLC destination. However, the DLC destination may describe only the current leg of a much longer journey. Because higher-level protocols embedded in the frame's data field have their own addresses, they may cause the recipient of the current frame to repack the data and retransmit it with a new address.

NOTE: Most topologies use six-byte addresses. ARCNET and LocalTalk, however, use one-byte addresses. On ARCNET, you can also enter addresses in octal rather than hexadecimal format or display DLC addresses in the octal format.

Defining Station Address Matches: Some Considerations

By defining station address matches, you can exercise considerable control over which frames are captured. The Sniffer analyzer evaluates the matches, starting with Match 1 (or the name you assign to Match 1) through Match 4. When a match succeeds, the analyzer stops testing for further matches. Whether or not the successful match is captured depends on whether you chose the **Include these** or **Exclude these** option associated with that match.

When none of the specified matches succeeds, the **Others** menu item determines whether the frames are captured anyway. **Include these** means the frames are captured; **Exclude these** means that they are not captured.

Using Fewer than Four Address Matches

It is not necessary to set all four matches; in fact, you may not want to set any at all. The analyzer disregards a match that contains only the default settings **From <any station>** and **To <any station>**. When all four matches are **From <any station> To <any station>**, the analyzer uses no address filters during capture.

Disabling Defined Address Matches

You can temporarily turn off the filter specified by a defined match by pressing Spacebar to disable (x) that match. The Sniffer analyzer checks only enabled matches marked with √.

Examples: Taking Advantage of Address Match Order

Suppose you are interested in all traffic to and from Server-1 except for the voluminous traffic between Server-1 and Gateway-A, which would quickly fill the capture buffer. Since the address filters are evaluated in sequence, you can define filters that first discard frames between Server-1 and Gateway-A and then accept frames between Server-1 and any other destination. The two sets of matches that would accomplish this are summarized in Figure 6–25.

	Match Name	Source Address	Destination Address	Reverse Direction	Include/ Exclude
Match 1	S1 to A	Server-1	Gateway A	yes	exclude
Match 2	S1 to others	Server-1	<any>	yes	include
Match 3	[Match 3]	<any>	<any>	[yes]	[include]
Match 4	[Match 4]	<any>	<any>	[yes]	[include]
Others					exclude

Figure 6–25. Address filter to capture all traffic—with one exception—from a station

Another example shows traffic between stations George or Anita and Server-1, as well as any traffic to Gateway-A (but not the reverse). To capture these frames, you could specify three matches as shown in Figure 6–26.

	Match Name	Source Address	Destination Address	Reverse Direction	Include/ Exclude
Match 1	G's files	George	Server-1	yes	include
Match 2	A's files	Anita	Server 1	yes	include
Match 3	Outgoing	<any>	Gateway A	no	include
Match 4	[Match 4]	<any>	<any>	[yes]	[include]
Others					exclude

Figure 6–26. Example of a filter match on three address pairs

Defining the Station Address Filters

After you determine what matches are required to capture the desired frames, you can define and name the matches that make up the station address filters.

To define station address capture filters:

1. Move to **Capture filters\Station address\Match 1** (Figure 6–27).

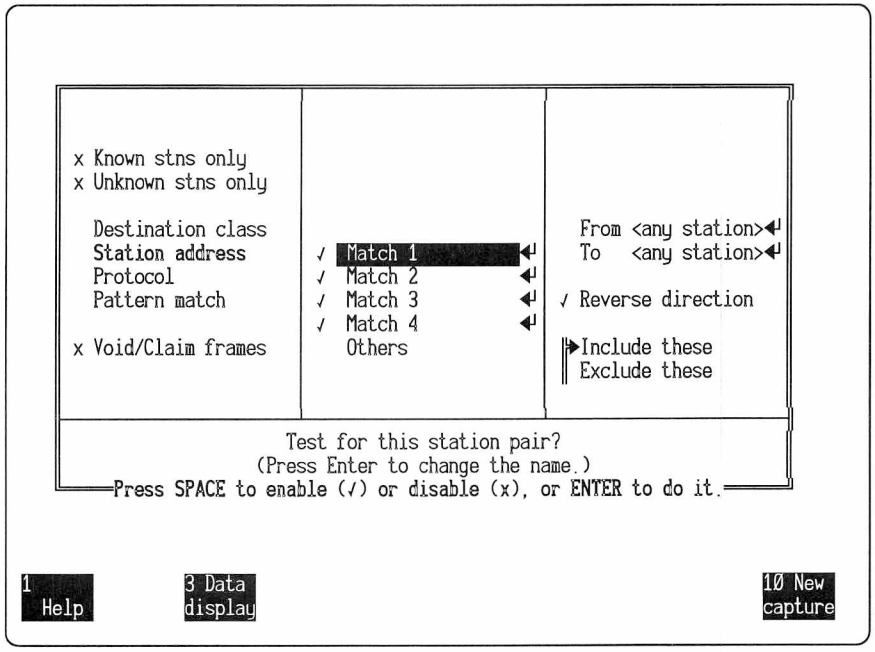


Figure 6–27. Defining a station address capture filter

2. If you want to name this match, press ENTER. In the dialog box that appears, type a name and press ENTER.
3. To specify a source address, move to **From** and press ENTER.

   In the table that appears (Figure 6–28), move to the desired station and press ENTER. If you enabled the **DLC addresses** option in the **Display\Summary** menu, the DLC address is automatically highlighted. If that option is disabled (the default) the highest level address is highlighted.

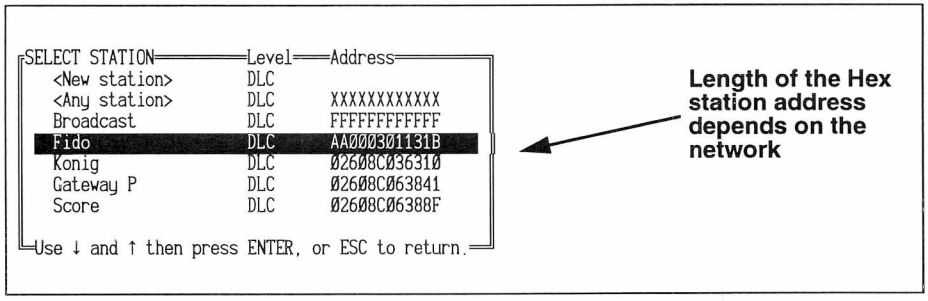


Figure 6–28. Selecting a station for a station address filter

Note that the address—either its name, if it has one, or the DLC address—replaces **<any station>** in the **From** menu item.

4. If the address you want is not in the table, move to **<New station>** at the top of the table and press ENTER.

   In the dialog box that appears (Figure 6–29), type a new DLC address and a corresponding symbolic name and press ENTER.

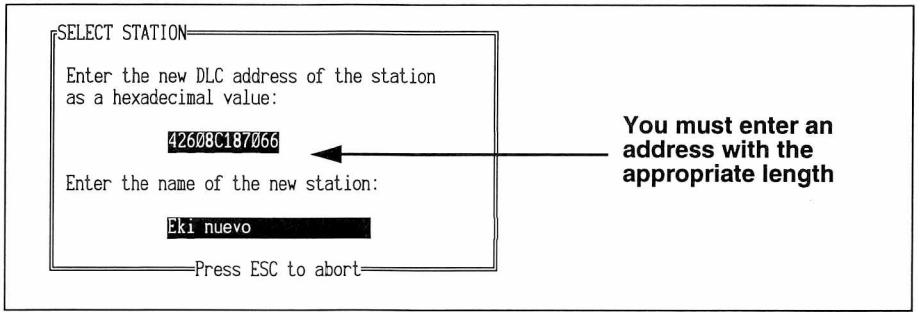

SELECT STATION
Enter the new DLC address of the station as a hexadecimal value:
42608C187066
Enter the name of the new station:
Eki nuevo
Press ESC to abort
You must enter an address with the appropriate length

Figure 6–29. Entering a new station address and name

5. To specify a destination address, move to **To** and press ENTER. Repeat the instructions in step 3 for selecting an address.

   As with the source address, the DLC address is automatically highlighted if you enabled the **DLC addresses** option in the **Display/Summary** menu. If that option is disabled (the default) the highest level address is highlighted. For ARCNET, you can enter the information as an octal value.

6. To specify whether this match also applies to traffic in the reverse direction, move to **Reverse direction** and press Spacebar to enable (√) or disable (x) the option.

7. To specify whether to include or exclude frames identified by this match, move to the appropriate option and press Spacebar to select the option you want.

   ▶ Include these
   Exclude these

8. Repeat steps 1 through 7 for up to four matches.

Protocol Filter

On a LAN, each DLC frame includes a field that indicates the frame type. Depending on the network, this low-level classification is called a *SAP* ("service access point" per IEEE 802.2) or an *Ethertype* (for Ethernet and StarLAN). This is the lowest level at which protocols are identified, which is also the only level available for capture filters. (Because the analyzer can devote more time to processing filters during the Display process, the display filters can include tests for higher-level protocols or addresses.)

Figure 6–30 shows some of the protocols available for capture filters. Next to each protocol, a √ indicates that the capture filter accepts that protocol, and an "x" that it

does not. The filter accepts a frame if it contains *any* of the protocols marked with a √. The default is all protocols enabled.

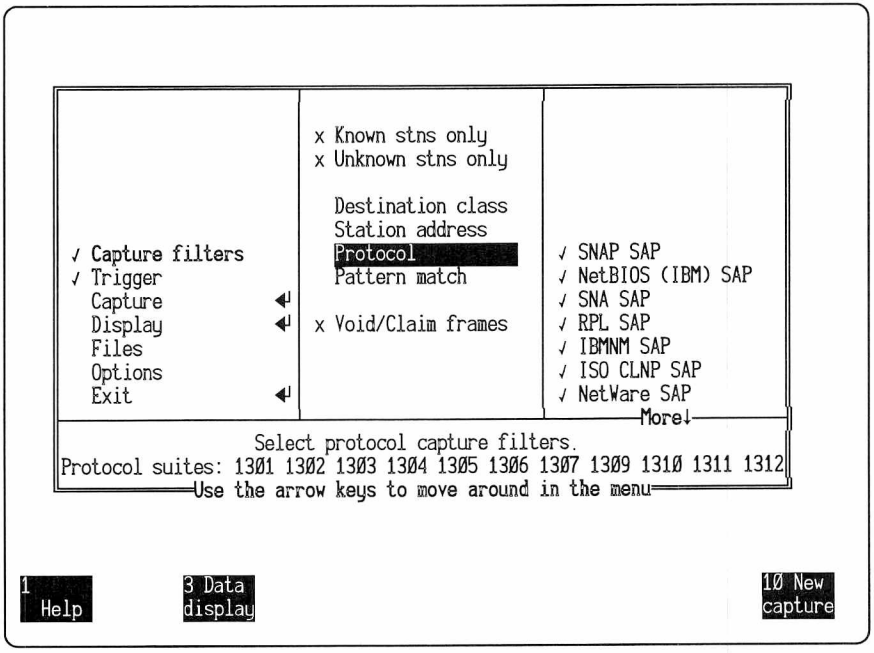


Figure 6–30. Defining the protocol capture filters

NOTE: Specific protocols available for capture filters on your Sniffer analyzer are listed in the **Capture filters** menu. Some typical protocol lists are shown in Figure 6–31.

Token Ring with IBM, XNS/MSNET, ISO, X.25	Ethernet with TCP/IP, Sun, DECnet, Banyan, AppleTalk, X-Window	Ethernet with IBM, Novell, XNS/MSNET, ISO, X.25	FDDI
√ MAC frames √ SNAP SAP √ BPDU SAP √ NetBIOS (IBM) SAP √ SNA SAP √ RPL SAP √ U-B SAP √ IBMNM SAP √ NetWare SAP √ ISO CLNP SAP √ XNS SAP √ X.25 SAP √ Other SAP	√ LOOP Etype √ 3Com Netmap Etype √ IP Etype √ ARP Etype √ TRLR Etype √ PUP Etype √ PUP ARP Etype √ SNMP Etype √ MOP Etype √ DRP Etype √ LAT Etype √ IP (VINES) Etype √ LOOP (VINES) Etype √ Echo (VINES) Etype √ ARP (Atalk) Etype √ LAP (Atalk) Etype √ Other Etype √ SNAP SAP √ BPDU SAP √ LLC (VINES) SAP √ Other SAP	√ LOOP Etype √ 3Com Netmap Etype √ IBMRT Etype √ NetWare Etype √ XNS Etype √ PUP Etype √ 3Com NBP Etype √ PUP ARP Etype √ Other Etype √ SNAP SAP √ BPDU SAP √ Net BIOS (IBM) SAP √ SNA SAP √ RLP SAP √ IBMNM SAP √ ISO/NetWare SAP √ X.25 SAP √ Other SAP	√ Void/Claim frames √ Other MAC frames √ SMT frames √ SNAP SAP √ NetBIOS (IBM) SAP √ SNA SAP √ RPL SAP √ IBMNM SAP √ ISO CLNP SAP √ NetWare SAP √ XNS SAP √ IP SAP √ LLC (VINES) SAP √ X.25 SAP √ Other SAP

Figure 6–31. DLC protocols typically available for capture filters

For most networks, the Sniffer analyzer's default setting is to accept every protocol.

Pattern Match Filter

A match consists of a pattern and the related offset. The pattern is a particular sequence of bits within a frame. The offset is the position of the bits within the data field of the frame. In a simple pattern, the bits occur at just one location. In a complex pattern, a set of up to eight simple component patterns is linked by AND/OR logic. The effect of NOT is achieved by choosing between **Match** and **Don't match**. The resulting set of patterns functions as a filter during capture.

Four Contexts for Pattern Matching

Setting up pattern matches as capture filters is only one of four contexts in which you specify a pattern as criteria for a function. The procedure for setting up these patterns is identical in all four contexts. However, a pattern established within one context has no effect on any other patterns.

The four contexts for pattern matching are:

Capture filter	The pattern that restricts which frames are accepted into the capture buffer during capture.
Trigger	The pattern that contains the "trigger" pattern, which stops the capture when it is detected.
Display filter	The pattern that restricts which frames in the capture buffer are displayed by the Display function.
Search	The pattern that specifies the search criteria for finding frames during display.

Because the Sniffer analyzer does not have time to invoke its interpreters for high-level protocols during capture, the analyzer cannot filter on high-level protocols or high-level addresses. However, it can execute fairly complex pattern matching. By experimenting with captured frames, you can often set up a pattern that, in effect, responds to a high-level embedded protocol.

Defining Complex Pattern Matches

By combining the four matches, you can define a complex pattern. The panel to the right of the **Pattern match** option contains the logical rules for combining the four component patterns into a set, as shown in Figure 6–32.

To help identify the four component patterns, you can assign each a name, which replaces the default names Match 1, Match 2, and so on. Note that these names don't affect processing; they simply identify each component pattern. To assign a name, move to Match 1 (or any other match), press ENTER, and type the name into the dialog box that appears.

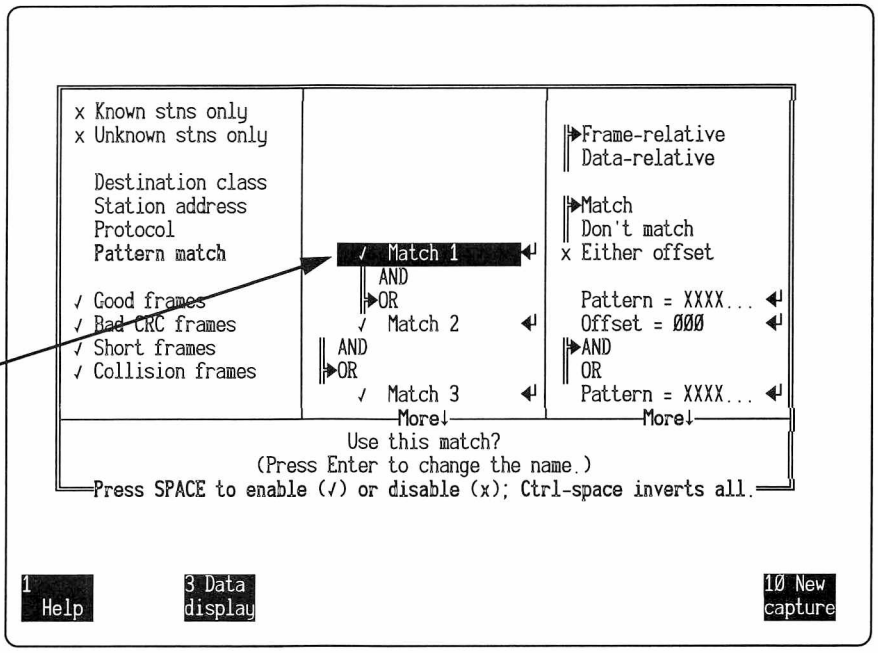


Figure 6–32. Defining a pattern match

Logical Combinations of the Four Matches

The four matches are combined by a logical AND or OR operator. The default is OR.

Matches are grouped into two sets of two, as shown in Figure 6–33. The analyzer first evaluates the relationship between Match 1 and Match 2, then between Match 3 and Match 4, and finally between the two pairs. Algebraically (with the symbol ⊗ standing for whichever relationship you set, either AND or OR), the relationship is summarized in this way:

(*Match 1* ⊗ *Match 2*) ⊗ (*Match 3* ⊗ *Match 4*)

The menu conveys this scheme by its pattern of indents.

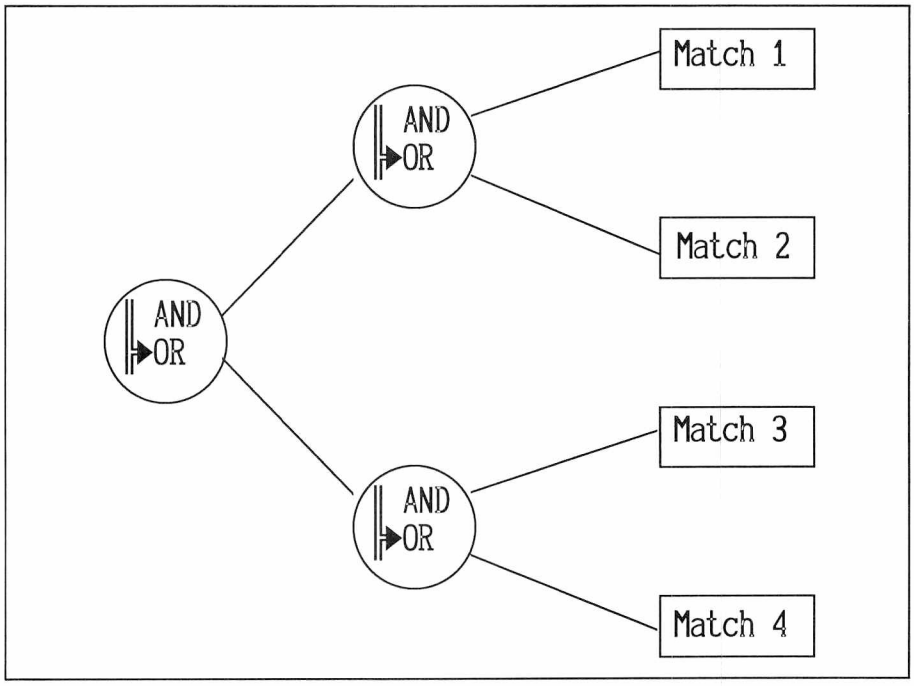


Figure 6–33. Combining four matches with AND and OR

Pairs of Patterns within a Match

Each individual match is composed of a pair of patterns that is linked by AND or OR logical operators. When you highlight a match name, the panel to the right shows its pair of component patterns. Initially, the default for all the individual patterns is X (null) and all the offsets are 00.

A pattern that consists of X characters has no effect. Therefore, you should set up only those patterns and matches you need. If you set up some matches but not others, it doesn't matter which matches you define and which you leave at the default settings.

Temporarily Disabling a Match

By default, all matches are enabled, with nulls in the pattern fields. By moving to a match and pressing Spacebar, you can temporarily disable (x) that match without deleting the defined pattern.

A Match on a Pair of Patterns

A single match can involve a pair of patterns (you may prefer to think of this as a pattern in two parts). In the menu, the two patterns appear one above the other, each

with its offset. You don't have to fill in both parts; any part you leave unspecified has no effect.

If you specify two patterns, you must also state the relationship between them: AND or OR. The default is OR. That is, to satisfy the match, the frame must contain *one* of the patterns.

For each pattern, you specify its location in the frame, which is called the "offset." Think of patterns as pattern A at offset *a*, and pattern B at offset *b*, resulting in the following match.

Pattern A at offset *a* AND Pattern B at offset *b*

Since these two patterns are in the same frame, a frame that meets this condition looks like Figure 6–34.

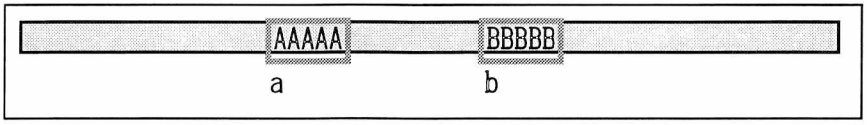


Figure 6–34. Frame containing both A at a *AND B at* b

When the relationship is OR rather than AND, either or both frames are acceptable, as shown in Figure 6–35.

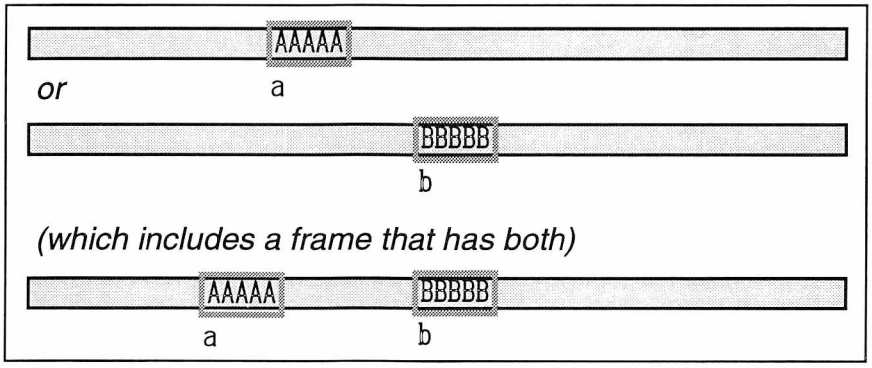


Figure 6–35. Frames containing either A at offset a OR B at offset b

Effect of the Either Offset Option

When you specify a pair of patterns, you can also enable the **Either offset** option. This usually makes sense only when the two patterns are related by AND. Figure 6–36 illustrates this concept.

For example, an exchange between a client and a server over TCP might involve the "well known port" number of the server and a transient port number assigned to the client. In the exchange, the port numbers occur at two different positions, corresponding to *source port* and to *destination port*. If the **Either offset** option is enabled for the patterns related by AND, frames that pass between these ports, in either direction, will be captured.

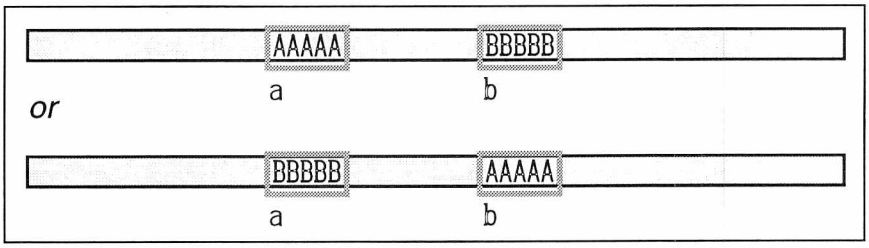


Figure 6–36. Effect of "Either offset" option when pairs are linked by AND

In the unusual case that OR *and* the **Either offset** options are enabled, any of the four frames shown in Figure 6–37 is a match. The filter specified by this combination would accept all traffic to and from port A, as well as all traffic to and from port B. That would include traffic between ports A and B, as well as all traffic with any other ports.

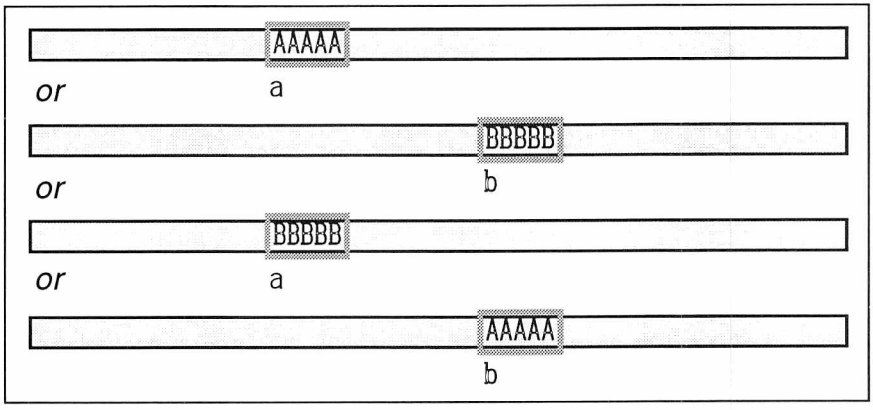


Figure 6–37. Effect of "Either offset" when pairs are linked by OR

Effect of the Match/Don't Match Option

For each of the four matches, you can choose between the **Match** or **Don't match** options.

This setting reverses the evaluation of each pattern within a match. The **Don't match** option is evaluated *before* the **Either offset** option and *before* the AND/OR logic that combines the pair. To see the effect of **Don't match**, replace "AAAAA" by

"Anything other than AAAAA" and replace "BBBBB" by "Anything other than BBBBB."

Whether the frame is accepted depends on the logic specified for combining the results of the four matches.

Examples

Suppose you describe a match as "pattern A at offset a." If you then enable **Don't match**, a frame should be accepted if, at offset a, it contains something *other than* pattern A.

When a match contains a pair of patterns linked by AND (for example, "Pattern A at offset a" *and also* "Pattern B at offset b"), enabling **Don't match** means that a frame should be accepted if it contains something *other than* pattern A at offset a *and* something *other than* pattern B at offset b.

When you specify a pair of patterns linked by OR (for example, "Pattern A at offset a" *or* "Pattern B at offset b"), enabling **Don't match** means that a frame should be accepted if it contains something *other than* "Pattern A at offset a" *or* something *other than* "Pattern B at offset b."

Characters and Offset in an Individual Pattern

Each individual pattern is defined by its position (offset) and the characters (or bits) it contains. A pattern may contain up to 32 characters.

Before you specify the pattern's content, first decide whether to enter it in hexadecimal, character, or binary format. The default is hexadecimal format.

Hexadecimal	Specify up to 16 bytes, each as a pair of hex digits 00 through FF.
Character	Specify up to 32 bytes, each as an ASCII character.
Binary	Specify up to 4 bytes as 32 binary bits, each a 0 or 1.

In hexadecimal or binary format, an X stands for anything at that position. In ASCII format, ALT-x has the same effect; when you press ALT-x, the corresponding position is shaded, like this: ▒.

Data-Relative vs. Frame-Relative Offset

The pattern's position within the frame is described by its *offset*. On token ring, FDDI, and certain other LANs, some frames contain a variable-length field called *source routing information* (RI). When this field is present, it appears after the DLC destination and source address, but before the regular data field.

As a result, the position of the data within a particular frame depends on whether that frame contains an RI field. When you specify the **Data relative** offset, the Sniffer analyzer adjusts the offset to compensate for the length of each frame's routing field. (For more information about the source routing field, see "About the Interpret RI Option" on page 3–5.)

If you are uncertain about whether a frame contains an RI field, you can define the offset in one of two ways:

Frame relative	Defines the offset as the number of bytes from the start of the frame.
Data relative	Defines the offset as the number of bytes from the start of the frame's data segment; that is, from the start of the 802.2 frame data.

When a frame's source and destination stations are on the same network, it requires no forwarding and the routing field is frequently, but not universally, omitted. If you are confident that all frames of interest are in the same format (either all contain an RI field or none do), it is safe to enable the **Frame-relative** offset option. Otherwise, enable the **Data-relative** offset option. Figure 6–32 shows these options in the menu.

Defining a Pattern Match Filter

To review: you can link up to four matches by AND or OR logical operators. You can define each match in hexadecimal, character, or binary format and determine its location in the frame by defining the offset, which can be data or frame relative. In addition, you can further define the pattern by enabling or disabling the **Either offset** option. You can also specify whether to include or exclude matches with the **Match** and **Don't Match** options. For more information about each of these options, review the earlier material in this section, starting with "Defining Complex Pattern Matches" on page 6–46.

Before defining a pattern match, first determine the pattern's logic with the options associated with the **Pattern match** filter. Figure 6–38 shows these options.

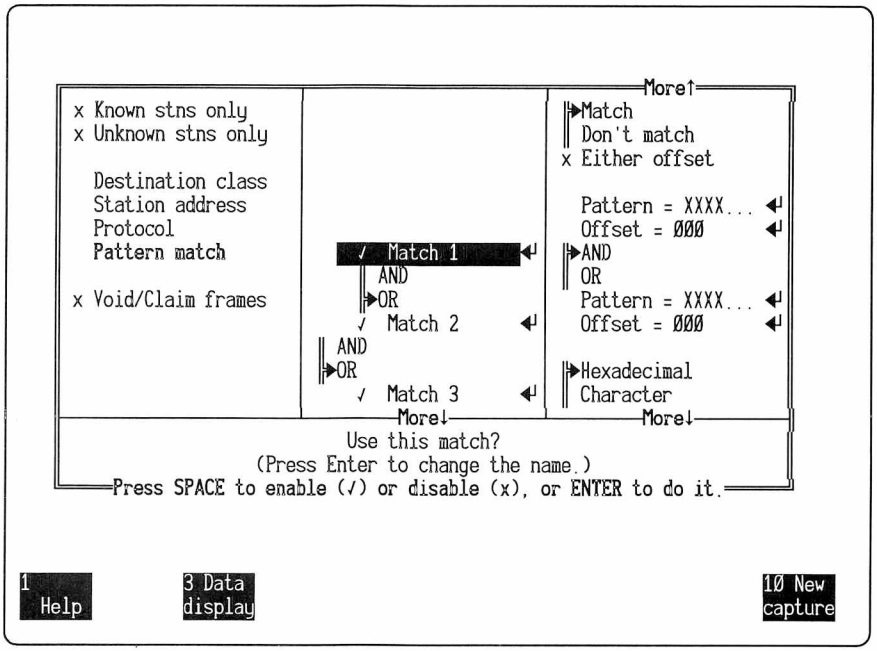


Figure 6–38. Defining a pattern match

To define a pattern match for a capture filter:

1. Move to **Capture filter\Pattern match\Match 1.**
2. If you want to name the match, press ENTER and type the desired name into the dialog box that appears.
3. Define the pattern's logic. Move to each of the desired options and press Spacebar to select that option.
   a. Define whether to compensate for the pattern's offset, depending on the presence of a source routing field.
   b. |▸ Frame-relative (default)
      ‖ Data-relative
   c. Define whether this match captures frames that either match or don't match the specified pattern.
   d. |▸ Match (default)
      ‖ Don't match
   e. Determine whether the offset of one of the patterns applies to the others. Move to the **Either offset** option and press Spacebar to enable or disable the option.

f. Determine the pattern's format (at the bottom of the panel).

```
▶ Hexadecimal (default)
  Character
  Binary
```

4. Specify the pattern.

   a. Move to **Pattern=** and press ENTER. In the dialog box that appears, type the pattern and press ENTER.

```
ENTER PATTERN
  Enter a pattern in hex, using X for don't-care:
    XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
                Press ESC to abort
```

   b. Move to **Offset=** and press ENTER. In the dialog box that appears, type the value of the offset and press ENTER. Note that the offset is always in hexadecimal.

```
ENTER BYTE OFFSET
  Enter a byte offset in hexadecimal:
    ____
                Press ESC to abort
```

5. Repeat steps 1 through 4 to define any other matches.
6. Define the relationship between the matches.

   a. For each match, press Spacebar to enable (√) or disable (x) that match.

   b. Define the logical relationships between Match 1 and Match 2, between Match 3 and Match 4, and between the two pairs of matches. For each, move to the desired option and press Spacebar.

```
  AND
▶ OR
```

Copying and Pasting a Pattern from the Display Hex Window

If you already captured a frame that contains the desired pattern, you can copy that pattern's characters and its offset, without having to type them again. (This procedure makes use of the Hex and Detail views chosen from the Display menu, as described in more detail in the next chapter.)

To enter a pattern by copying and pasting:

1. Move to **Display\ Detail** and **Display\Hex** and press Spacebar to enable both options. Press F9 **[Pause]** and then F3 **[Data display]** to display the interpreted frames.
2. Find the frame that contains the pattern you want.
3. In the Detail view, move to the desired field. This automatically highlights the corresponding field in the Hex view.
4. While the field is highlighted, press F5 to return to the main menu.
5. Move to **Capture filters\Pattern match** and then to one of the four matches.
6. If necessary, move up to define the **Frame-relative** or **Data-relative** offset options.
7. Move to **Pattern=** and press ENTER to display the associated dialog box.
8. Press the CURSOR UP key. In response, the analyzer copies the characters highlighted in the Hex view into the pattern entry dialog box. Press ENTER to record the pattern.
9. Move to **Offset=** and press ENTER. Press the CURSOR UP key to copy the pattern's offset into the offset dialog box. Press ENTER to record the offset.

Example of a Capture Filter Pattern Match

The following example is based on the use of Telnet over TCP/IP over Ethernet, using the sample file TCPIP.ENC in the CAPTURE directory. However, the general strategy for setting a pattern match is not specific to the network or protocols of this example.

Suppose you experience a problem while using a terminal emulation package. While connected to a remote host, the network software confuses the actions of the BACKSPACE and DELETE keys, which (in this application) are supposed to do different things. Who is mixing them up? The emulator at the PC? The application at the host? The network software between them?

As a first step, you might examine what the emulator transmits to the host when you press BACKSPACE and when you press DELETE, as well as what the host echoes back for each character. (Telnet often supports a terminal by transmitting one character at a time to the host. Usually, the host echoes each displayable character back to the terminal one at a time.)

To study what happens, you need a filter that accepts only those frames that include either BACKSPACE or DELETE embedded in a Telnet frame passing between the host and the terminal emulation program. Although you can't set a capture filter for the Telnet protocol explicitly (since you can't filter on high-level protocols during capture), you can achieve the same result with pattern matching. Here's how you discover a pattern that identifies not just a Telnet frame, but one whose content involves the characters in question.

First, set an address filter to select all frames sent from the terminal emulator. Then (from the terminal emulator) execute a command that uses BACKSPACE and then a command that uses DELETE. By browsing through the frames thus captured, you can readily find Telnet frames addressed to the host. By examining the captured frames, you can see that each consists of:

- A DLC frame (with a DLC source, destination, and IP ethertype), and within that
- An IP frame (with an IP source, destination, and TCP protocol), and within that
- A TCP frame (with a TCP source and destination port of "Telnet"), and within that
- A Telnet frame that contains the record of a keystroke sent from the terminal emulator to the host

To study how the program treats BACKSPACE and DELETE, you can use the "copy and paste" facility to set a capture filter to accept a frame that matches the following pattern:

- It contains the IP protocol number for "TCP" (hex "06" at offset 17).
- It contains the TCP code for Telnet data (indicated by a TCP source or destination port number of hexadecimal 17).
- Its IP source is the address of the PC running the terminal emulator, and its IP destination is the address of the host, or vice versa (by checking either offset).
- The Telnet data is either the code for delete (7F) or the code for backspace (08).

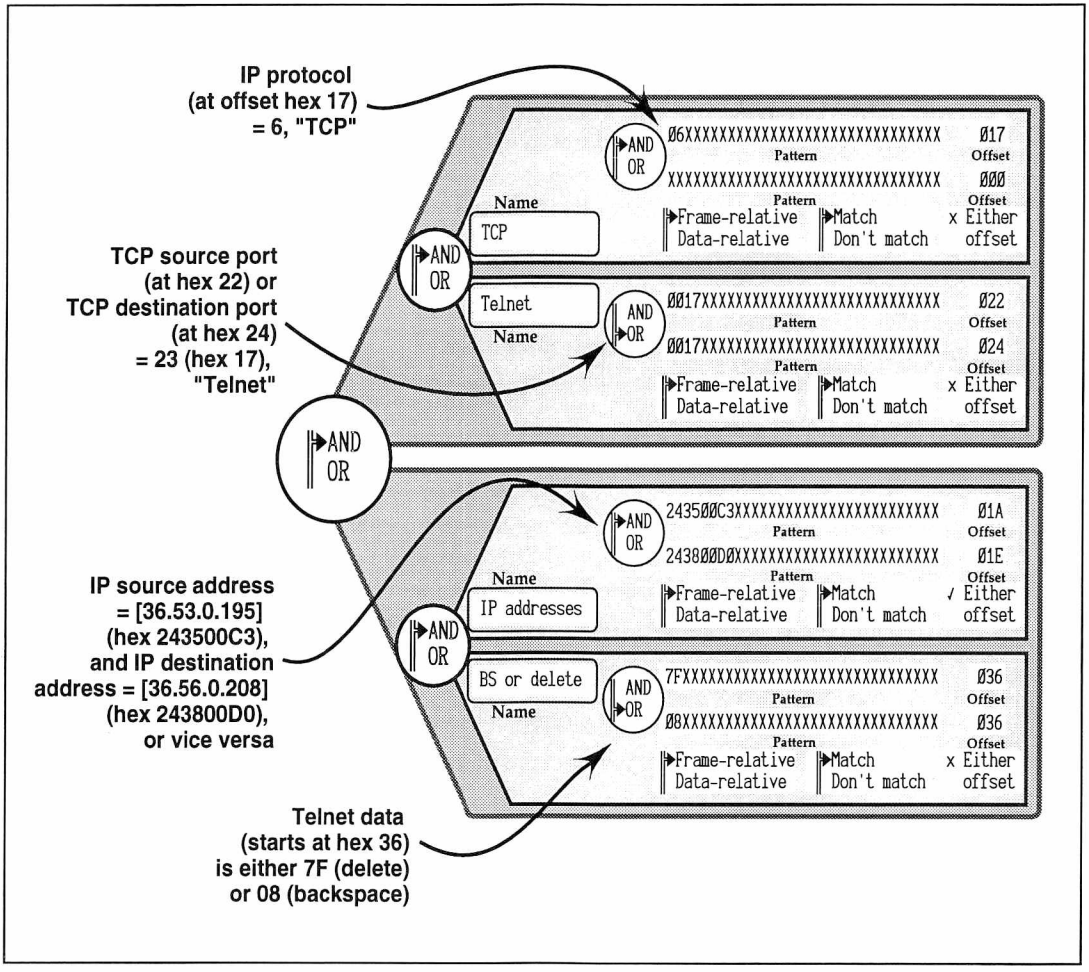


Figure 6–39. Example of a pattern match in the capture filter

Figure 6–39 is based on the sample file TCPIP.ENC in the CAPTURE directory. It shows how pairs of individual patterns are combined to create matches, and how the resulting matches are combined to create the filter. The shading shows how various components are grouped. The fields show the data for the example. (Of course, in a real situation, the IP addresses would be different, but the values for "Telnet" and "TCP" are appropriate.)

Void/Claim Frames Filter

On FDDI networks, this filter checks for the presence of void or claim frames. When enabled, the Sniffer analyzer captures void and claim frames. When disabled, the

analyzer ignores these frames. Note that this is a hardware filter and only works on live capture. This filter is not applicable to trace file replay.

Claim frames are used in the "claim process" as part of the ring initialization process. The claim process begins when a station's MAC entity transmits claim frames (containing the station's address and bid for the target token rotation time). Other stations in the ring compare the claim frames with their own. When a station receives its own claim frame, it wins the right to initialize the ring.

Void frames are frames that contain no data, though they contain starting and ending bits.

The default is **x Void/Claim frames** disabled.

Filters for Defective Frames

On a WAN/Synchronous link and on Ethernet, StarLAN, and PC Network topologies, the Sniffer analyzer can filter frames for either the presence or absence of certain defects. Note that this ability is available only if the adapter card retains defective frames and passes them to the analyzer's CPU. The adapter card for token ring simply discards defective frames, so you cannot filter for defective frames.

The breakdown for Ethernet frames includes:

- **Good frames** that contain none of the other defects
- **Bad CRC frames**, which include frames found to be defective by the cyclic redundancy check (CRC)
- **Short frames**, which include frames shorter than 60 byte
- **Collision frames** (Ethernet-II only), which indicate the results of a collision

How the Defective Frames Filters Work (Ethernet)

Figure 6–40 shows the normal collision window and late collisions that occur after byte 64. Within the normal collision window, there is the preamble area and the frame area. Whether collisions in each of these areas are counted and whether—and how—the associated frames are flagged depends on whether your Sniffer analyzer has an Ethernet or Ethernet-II adapter card.

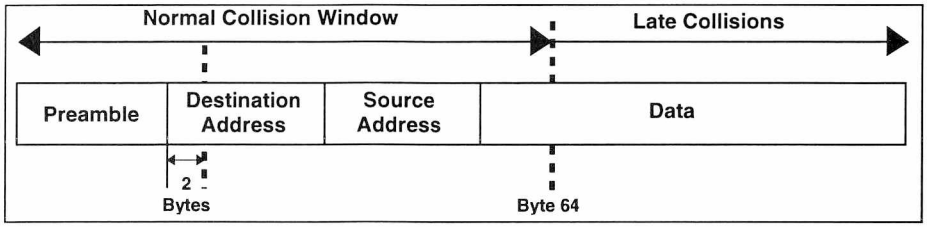


Figure 6–40. Collision detection

For analyzers with an Ethernet adapter card, collisions in the preamble are neither counted nor flagged. Collisions after the first two bytes of the frame area are counted as short frames and flagged "R" (runt). Collisions after byte 64 are counted as CRC errors and flagged "C" (CRC).

For analyzers with an Ethernet-II adapter card, collisions in the preamble are counted, but the frames are *not* stored in the capture buffer. Collisions in the frame area are counted as collision frames and flagged "X" (Collision). Collisions after byte 64 are also counted and flagged "X."

Figure 6–41 provides an overview of how collision frames are treated by the two networks.

	Ethernet		Ethernet-II	
Collision detected in...	**counted**	**flagged**	**counted**	**flagged**
Preamble	no	no	yes	not stored
Frame area	yes	R (Runt)	yes	X (Collision)
Late collision	yes	C (CRC)	yes	X (Collision)

Figure 6–41. Overview of how collision frames are treated

NOTE: Because collisions that occurred in the preamble area (or the first two bytes of the frame area) are not followed by frame data, you will not be able to see the collision frames even though they are counted. Since many collisions occur in the preamble area of the frame, this is a common occurrence.

Defective Frames on an FDDI Network

The capture filters for an FDDI network do not provide separate choices for the various kinds of defective frames. They are simply referred to as error frames. When

you enable **Error frames** from the **Capture filters** menu, the capture will include these types of error frames:

E-flag set	Another station has marked this frame as an error frame by setting the frame's E-flag.
Bad CRC	The analyzer detected the bad CRC. In accordance with the FDDI standard, the analyzer will set the frame's E-flag.
Fragment frame	The analyzer detected the fragment frame and will decode the frame as having invalid frame status.

Sniffer Internetwork Analyzer Capture Filters

When capturing traffic on a WAN/Synchronous link, the following capture filters are available:

- Pattern match
- From DTE
- From DCE
- RR frames
- RNR frames
- Info frames
- Good frames
- Bad CRC frames

The **Pattern match**, **Good frames**, and **Bad CRC frames** filters are the same as those for LANs. For additional information, see "Pattern Match Filter" on page 6–45 and "Filters for Defective Frames" on page 6–58.

From DTE/From DCE Capture Filters

The **From DTE** (Data Terminal Equipment) and **From DCE** (Data Communication Equipment) filters allow you to filter on direction. Although the WAN/Synchronous link is bidirectional (**From DTE** or **From DCE**), you can choose to accept frames in just one, the other, or both directions. You can also set both **From DTE** and **From DCE** to off (x). However, if you do this, no data will be captured.

RR Frames/RNR Frames Capture Filters

You can also filter for **RR** (Receiver Ready) and **RNR** (Receiver not Ready) frames. These frames are exchanged by the DTE and DCE devices in the process of setting up communications between the endpoints of a WAN/Synchronous link. Once the link

is established, these frames control the flow of frames. Therefore, if you are investigating problems in handshaking or flow control, these filters may be relevant. When you are interested primarily in the higher-level messages, the RR and RNR frames are usually irrelevant.

Info Frames Capture Filter

The **Info frames** capture filter allows you to filter on SDLC/HDLC Info frames (commonly called "I-frames"). Info frames carry the actual data to be transmitted for the user. Additionally, SDLC/HDLC Info frames can carry flow and error control data, and as such, may be useful for troubleshooting problems on the WAN link.

To set the Sniffer Internetwork Analyzer capture filters:

1. Move to **Capture filters** and then to the desired filter.
2. Press Spacebar to enable (√) or disable (x) the desired filter, as appropriate. For example:
   √ From DTE
   √ From DCE

Stopping Capture

You can always stop a capture in progress by pressing F10 **[Stop capture]**. However, instead of randomly stopping capture and risking losing frames when the buffer fills, you can also stop capture automatically in one of two ways:

- When the buffer is full
- When the Sniffer analyzer detects a trigger event

You can either enable or disable the automatic **Stop capture** feature. If you choose to stop capture automatically, you can further define whether to stop when the buffer is full or when the trigger event is detected. You can also save all or a portion of the capture buffer that contains the trigger event to the hard disk.

To determine how to stop the capture:

1. Move to **Trigger\Stop capture** and then to the desired option.
   ▶ Stop at trigger
   Stop when full
2. Press Spacebar to enable (√) that option.

Defining a Trigger to Stop Capture

If you enabled the **Stop at trigger** option, the Sniffer analyzer automatically stops capture when it detects a *trigger event*, which can be either an internal or external trigger.

An internal trigger can be a specified defective frame (on WAN/Synchronous links and on Ethernet, StarLAN, and PC Network topologies) or a frame that contains a pattern you specify. An external trigger occurs when the analyzer detects a signal at its serial port. Such a signal is typically sent by another computer, which is linked to the analyzer with a serial port to serial port connection, or by a sensor connected to the port. In addition, the analyzer can send a signal to the port when the trigger event occurs. This signal could notify another computer or device connected to the serial port.

When the trigger event occurs, the capture either stops immediately or after a specified delay. As a result, the capture buffer contains the *trigger frame*, the frame that preceded the trigger frame, and (optionally) the frames that followed it. The word "TRIGGERED" replaces the word "CAPTURING" in the top left of the capture screen. You can see this in Figure 6–42.

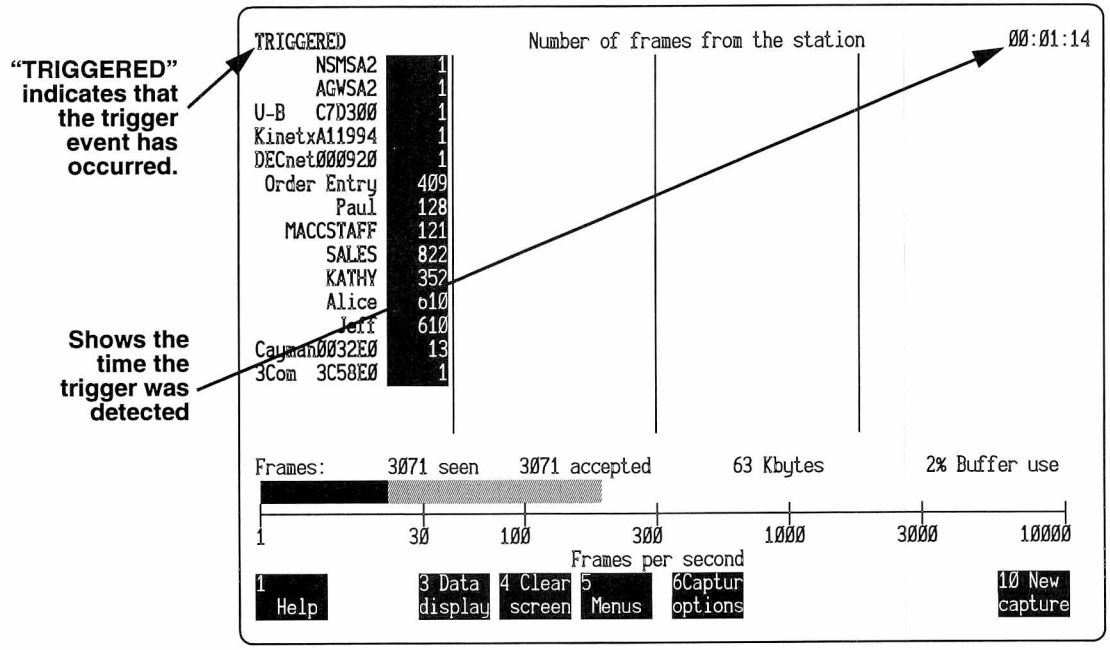


Figure 6–42. Indication that capture is stopped by trigger event

When you display the contents of the capture buffer, the trigger frame is marked with the letter "T" when later displayed in the Summary view (see "Flags Display Option"

on page 7–40). You can use this flag to search for the trigger frame and to display the time relative to its arrival (see "Searching for Frames" on page 7–55).

Note that the capture buffer never contains more than one frame marked T. Even if a second frame with the trigger pattern arrives during the delay before capture is stopped, only the first frame is reported and flagged as the trigger.

Setting a trigger consists of three tasks:

- Defining the trigger event
- Determining whether to save the portion of the capture buffer that contains the trigger frame to disk (disk snapshot)
- Defining the delay after the trigger event at which capture stops

As with the capture filters, you can temporarily prevent a trigger pattern from stopping capture by disabling the **Trigger** option.

Defining the Trigger Event

Defining a trigger event that consists of defective frames (on most LANs or on WAN/Synchronous links) or of an external trigger is relatively straightforward. Defining a trigger that consists of a pattern match requires more planning and perhaps some experimentation. For detailed information about defining pattern matches, refer to "Defining Complex Pattern Matches" on page 6–46.

The FDDI analyzer allows you to use Error frames as the trigger event.

You can also use the Expert analyzer's diagnoses as trigger events. For information on this capability, see "Expert Triggers" on page 6–69. If you set both classic and Expert triggers, make sure you read "The Order in Which the Analyzer Processes Triggers" on page 6–73.

Figure 6–43 shows the options associated with defining the trigger for an Ethernet-II Sniffer analyzer.

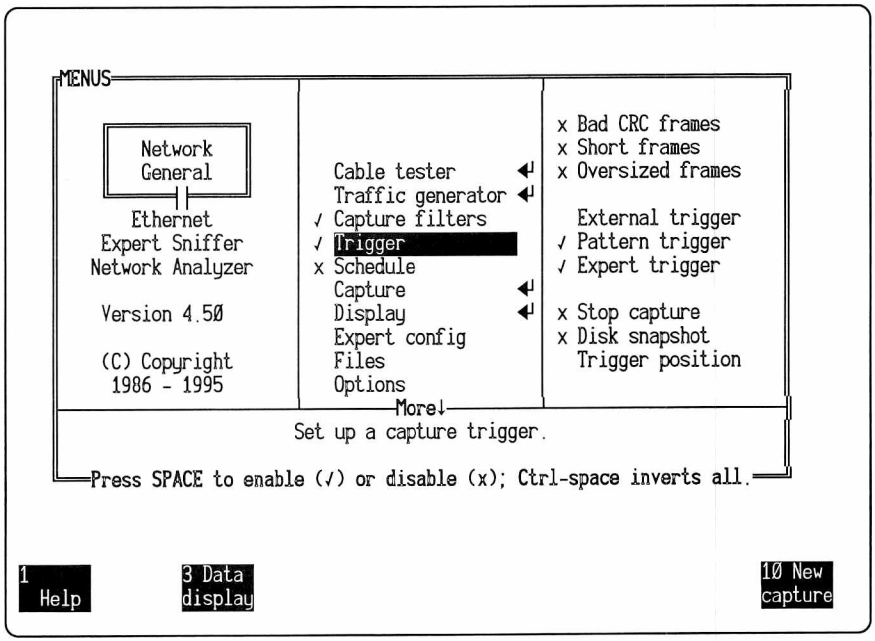


Figure 6–43. Trigger menu for an Ethernet-II analyzer

To define the trigger event on a LAN:

1. Move to **Trigger \ Stop capture \ Stop at trigger** and press Spacebar to choose the desired option.

   ▶ Stop at trigger
   Stop when full

2. To define an external trigger, move to **Trigger \ External trigger** and press Spacebar to enable (√) the desired options.

   x From COM1 CTS/DSR
   x To COM1 RTS/DTR

   If you are using a serial mouse, you cannot use the external trigger.

3. To define defective frames as the trigger event on Ethernet, StarLAN, or PC Network, press Spacebar to enable (√) the desired options.

   √ Bad CRC frames
   x Short frames
   x Oversize frames (Ethernet only)
   x Error frames (FDDI only)

4. To define a pattern as the trigger event, define up to four matches. For each match, press Spacebar to set up the desired pattern.

   √ Match 1
   ‖ AND
   ‖► OR
   √ Match 2
   ‖ AND
   ‖► OR
   √ Match 3
   ‖ AND
   ‖► OR
   √ Match 4

Examples of Pattern Match Triggers: LAN

Figure 6–44 shows two examples of how to use pattern matches as a trigger to stop capture.

Token Ring/IBM	Ethernet/XNS (3Com + network)
To trigger on a frame reporting an SMB error, first set the capture filter to pass only NetBIOS frames. Then set the trigger to stop the capture when it finds that the primary SMB return code is not equal to 00 (zero means "Classic"). In an IBM SMB frame, the primary return code is a single byte located at data relative offset 27 (hex).	To trigger on a frame reporting an SMB error, first set the capture filter to pass only XNS frames. Then set the trigger to stop the capture when it finds that the primary SMB return code is not equal to 00 (zero means "Classic"). In an XNS SMB frame, the primary return code is a single byte located at data relative offset 3D (hex).

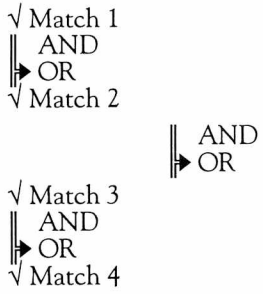
Figure 6–44. Sample trigger pattern matches on token ring and Ethernet networks

To define the trigger event on a WAN/Synchronous link:

1. Move to **Trigger\Stop capture\Stop at trigger** and press Spacebar to enable (√) the option.
2. To define **Bad CRC frames** as the trigger, move to that option and press Spacebar to enable (√) it.
3. To define an external trigger, move to the desired options and press Spacebar to enable or disable the options.

   √ From COM1 CTS/DSR
   √ To COM1 RTS/DTR

4. To define a pattern as the trigger event, define up to four matches. For each match, press Spacebar to set up the desired pattern.



Saving the Trigger Frame to Disk

The **Disk snapshot** option, when enabled, lets you save the portion of capture buffer that contains the trigger frame as a file on the analyzer's hard disk, to examine its contents later. As each snapshot file is saved, the system assigns it the name "Snap", a number from 1 through the maximum number you defined (the default is 10), and an extension that identifies your network. For example, the fourth snapshot on an Ethernet network would be named "SNAP4.ENC". These files are stored in the CAPTURE directory.

The options associated with the **Disk snapshot** option include:

- Whether to save when the snapshot file is full or when the trigger event is detected. If you choose the **Save when full** option, the buffer is saved continuously (whether the trigger event is detected or not) until you reach the maximum number of snapshot files, unless the **Overwrite files** option is enabled.
- The size of the snapshot file.
- The maximum number of snapshot files to be created.
- Whether to overwrite existing snapshot files when you exceed the maximum specified by the **Files =** option.
- Whether to save the snapshot files in compressed format. This process is transparent to the analyzer. That is, when you play back files saved in compressed format, they will be automatically decompressed by the analyzer. Note, however, that compressed files cannot be decompressed by earlier (pre-4.30) versions of the analyzer software.

How much information is saved in the snapshot files also depends on the **Trigger position** you specify, which determines the delay after the trigger event before the capture stops. This determines how many of the frames that surround the trigger frame are captured. This option is explained in more detail in the next section.

To save snapshot files to disk:

1. Move to **Trigger\Disk snapshot.** Press Spacebar, if necessary, to enable (√) the option.
2. Determine when to take the snapshot. If you choose **Save when full**, how much is saved depends on the size you specify for the snapshot file.

   ▶ Save at trigger
   Save when full
3. To change the size of the snapshot files, move to **Size=** and press ENTER. In the dialog box that appears, type the desired file size and press ENTER. Figure 6–45 shows this dialog box.

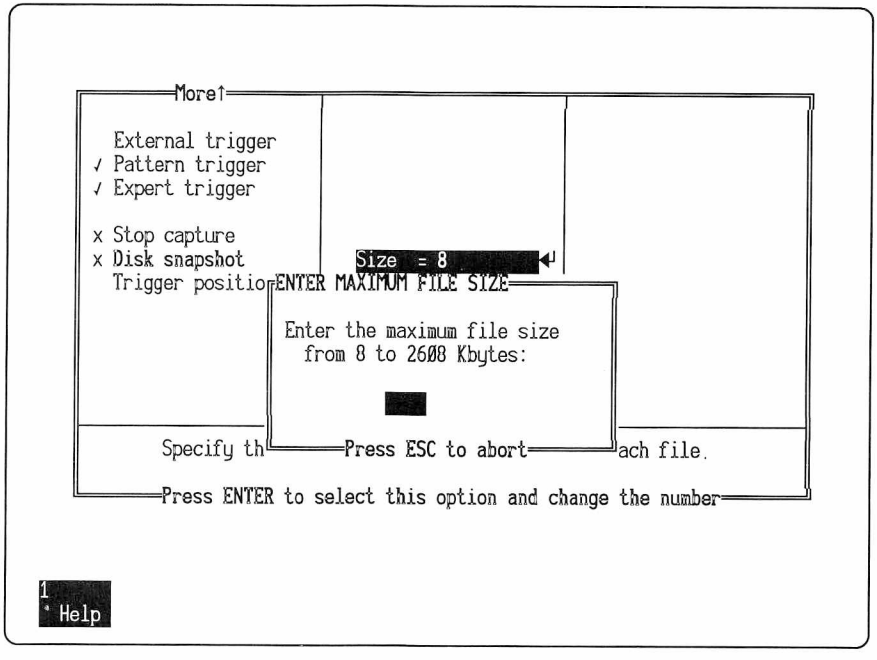
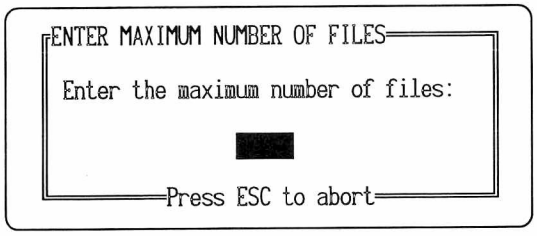


Figure 6–45. Defining the size of snapshot files

4. To change the maximum number of snapshot files created, move to **Files=** and press ENTER. In the dialog box that appears, type the desired maximum number of files and press ENTER.



5. To determine how to handle files that exceed this maximum, move to **Overwrite files.** Press Spacebar to enable (√) or disable (x) the option.
6. To determine whether the files are saved compressed or uncompressed, move to **Compress files.** Press Spacebar to enable (√) or disable (x) the option.

Defining the Trigger Delay

The **Trigger position** option determines whether capture stops immediately when the trigger event is detected or after some delay. By setting a delay, you can retain the frames that precede or follow the trigger event.

The effects of the various stopping options are summarized in Figure 6–46.

Option	Effect
Stop when full	Even if the trigger event has not occurred, capture stops when there is no more space in the capture buffer.
Continuous capture	The frames that arrived earlier are discarded to make room in the capture buffer for the newer arrivals. When the trigger event occurs, the analyzer (as usual) posts the word "TRIGGERED" on the screen, but does not stop capturing. If nothing else happens to stop capture, sooner or later—depending on the size of the frames and the space in the buffer—arriving frames will displace those already captured and the trigger frame will be among those discarded.
0% pretrigger	Capture continues until the trigger frame is the oldest remaining in the capture buffer (frame 1), and all other frames follow it.
25% pretrigger	Capture continues until 25% of the space in the capture buffer is devoted to frames that arrived before the trigger frame.
50% pretrigger	As above, but 50% of the space in the capture buffer is devoted to frames that arrived before the trigger frame.

Figure 6–46. Effect of "stop capture" options in the trigger menu

75% pretrigger	As above, but 75% of the space in the capture buffer is devoted to frames that arrived before the trigger frame.
100% pretrigger	Capture stops at once, so that the trigger frame is the last to arrive in the capture buffer and all other frames preceded it.

Figure 6–46. Effect of "stop capture" options in the trigger menu

To define the trigger delay:

1. Move to **Trigger\Trigger position.**
2. Determine when to stop the capture. Move to **Stop at capture** and then to the percentage of frames saved before the trigger was detected. To select one, move to the desired option and press Spacebar.

```
0% pretrigger
25% pretrigger
50% pretrigger
75% pretrigger (default)
100% pretrigger
```

Temporarily Disabling the Trigger Option

As with the capture filters, you can temporarily disable the defined trigger without changing the trigger options you defined. In that way, you don't have to undo your work. This is especially useful if you defined a complex match pattern as the trigger event.

Expert Triggers

Expert triggers allow you to use diagnoses as trigger events, anchoring capture to make sure the frames that interest you are either saved to hard disk as a snapshot or remain in the capture buffer. This section describes the mechanics of setting an Expert trigger. It does not discuss in detail the meanings of the triggers, which are described in the next few sections.

IMPORTANT: You can specify an Expert trigger along with external and pattern triggers. If you use these different types of triggers, you should read "The Order in Which the Analyzer Processes Triggers" on page 6–73 to understand how the analyzer processes triggers.

To set an Expert trigger:

1. Use the cursor keys to move to the **Trigger\Expert Trigger** menu.

2. Move the highlight to the layer at which you want to specify an Expert trigger.
   Result: A list of Expert triggers associated with the highlighted layer appears in the right menu panel. Figure 6–47 shows the Expert triggers associated with the Application layer.

In Figure 6–47, notice that each Expert trigger is preceded by either an x or a √. Triggers preceded by a √ are enabled; those preceded by an x are disabled. You can use the Spacebar to toggle between enabled/disabled. By pressing CTRL-Spacebar, you can reverse all selections in the current display.

3. Move the highlight to a trigger you want to enable. Press the Spacebar to change its tag from an x (disabled) to √ (enabled). Repeat this process for each trigger you want to enable or disable. In Figure 6–47, the Expert trigger **Slow server** is enabled.
4. In Figure 6–47, the menu item **Expert trigger** is also preceded by a √. You can enable or disable all Expert triggers as a group.
5. Set other trigger options, such as **Stop capture**, **Disk snapshot**, and **Trigger position**. For more information on these options, see the preceding sections.
6. Press F10 **[New capture]** to start capture.
   Result: When capture begins, the new trigger takes effect.

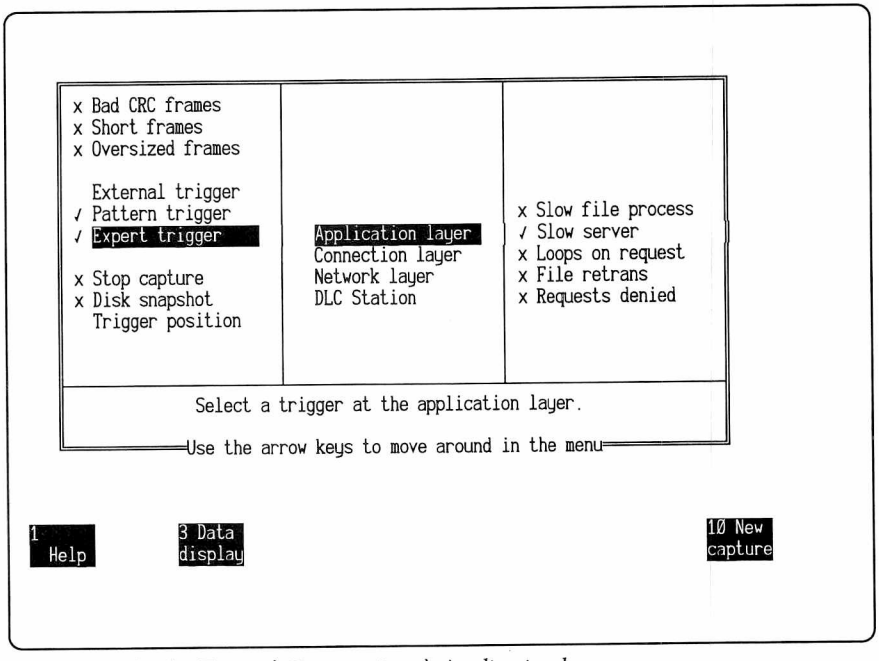


Figure 6–47. The Trigger\Expert trigger\Application layer menu

Effects of an Expert Trigger

The frame causing an Expert trigger is marked with a T in the summary view. The diagnosis was probably not caused by the marked frame alone. The mark simply indicates where the diagnosis is made. For example, if you set the diagnosis **Broadcast storm** to be the trigger event, the trigger frame indicates at what time the analyzer decided that a broadcast storm happened; it doesn't mean that the frame itself caused a broadcast storm.

After an Expert trigger occurs, the analyzer does the following:

- Emits a beep, notifying you that a trigger event has occurred.
- Continues or stops capture, depending on the settings of **Stop capture** and **Trigger position**.

  If **Stop capture** is disabled, the analyzer continues capturing, and it is possible that the frame associated with an Expert trigger could be pushed out of the buffer by the time you stop capture.

  If **Stop at trigger** is selected, the analyzer continues capturing until the frame associated with the Expert trigger is in the position described by **Trigger position**. For example, if **Trigger position** is 100 percent pretrigger, capture stops immediately after the trigger event has happened.

  If **Stop when full** is selected, the analyzer continues capturing until the buffer is full. If a trigger event occurs, the trigger frame remains in the buffer, but its relative position is not predetermined.
- If **Disk snapshot** is selected, the analyzer stores the frames surrounding the trigger event to the disk. Depending on the configuration of the various **Disk snapshot** options, the analyzer can either continue capturing or stop after the first trigger.

Available Expert Triggers

The Expert triggers are organized by Expert layers, each of which contains several trigger options. Figure 6–48 summarizes the Expert triggers available at each Expert layer.

Expert Layer	Expert Threshold
Application Layer	Slow file process
	Slow server
	Loops on request
	File retransmission
	Requests denied
Connection Layer	Broken connection
	Retransmission
Network Station Layer	Duplicate address
	Local router
	Multiple routers
	Subnet down
	Bad routing table
	Subnet conflict
DLC Station Layer	Overloaded LAN
	Broadcast storm
	Physical error
	Overloaded WAN
	WAN underload*
	HDLC retransmits*
	Overcongested WAN*
	Underload congestion*
MAC Layer (Token Ring)	Token ring entry
	Ring purge
	Receiver congestion
	Station removed
	Beaconing ring
	Token ring burst

*Sniffer Internetwork Analyzer (WAN/Synchronous) only

Figure 6–48. The Trigger\Expert trigger\Application layer menu

The Order in Which the Analyzer Processes Triggers

Normally, if you specify multiple triggers, whichever frame that fulfills a trigger condition first is considered the trigger frame and is marked with a T.

However, if you specify both Classic and Expert triggers, it is possible that the analyzer will ignore the Expert trigger event even though it precedes the Classic event. This is because the analyzer processes Classic triggers faster than Expert triggers. The following example explains this concept.

Example: Processing Expert and Classic Triggers

Suppose you specify one Classic pattern-match trigger and one Expert trigger. In Figure 6–49, frame 90 fulfills the condition of the Expert trigger and frame 100 fulfills that of the pattern-match trigger. Because the analyzer processes the Classic pattern-match trigger on frame 100 before it performs Expert analysis on frame 90, frame 100 is marked as the trigger frame instead of frame 90. The analyzer does not consider frame 90 to be the first trigger event. As a result, you might not be aware that a frame associated with the Expert trigger has ever occurred.

IMPORTANT: You can avoid this problem by enabling only Expert triggers. If no Classic triggers are enabled, you are assured that the analyzer will recognize the Expert trigger event accurately.

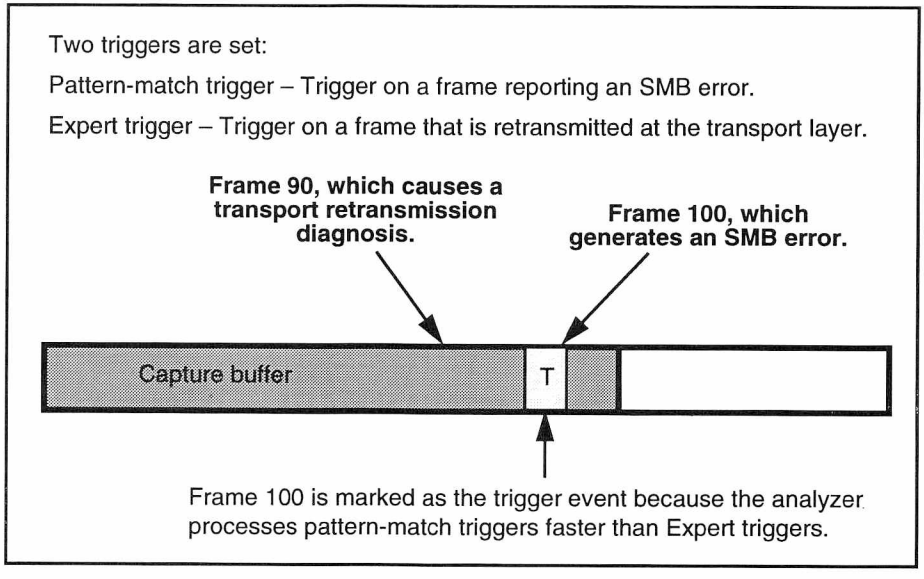

Two triggers are set:
Pattern-match trigger – Trigger on a frame reporting an SMB error.
Expert trigger – Trigger on a frame that is retransmitted at the transport layer.
Frame 90, which causes a transport retransmission diagnosis.
Frame 100, which generates an SMB error.
Capture buffer
T
Frame 100 is marked as the trigger event because the analyzer processes pattern-match triggers faster than Expert triggers.

Figure 6–49. The order in which the analyzer processes triggers

Starting the Capture

After you set the capture mode, various capture options, the capture filters, and the trigger, you are ready to start the capture.

To start capture:

1. Make sure all options are defined correctly.
2. Press F10 **[New Capture]**. Or, in the main menu, move to **Capture** and press ENTER.

   The Sniffer analyzer starts to capture frames. The screen shows the progress of the capture in the screen format you specified (individual counts, pair counts, or skylines).

Pausing or Stopping Capture

Once started, capture continues until one of the following happens:

- You press F10 **[Stop capture]** to stop capture.
- The specified trigger event occurs (if you enabled **Stop capture\Stop at trigger**).
- The capture buffer is full (if you enabled **Stop capture\Stop when full**).
- You press F9 **[Pause capture]** to pause capture. This permits you to adjust the screen format or the capture filters and then resume the capture.

What You Can Do While Capture is Paused

If you press F9 **[Pause]**, the Sniffer analyzer pauses the capture. Frames are no longer captured, but the frames already captured remain in the capture buffer. At this point, you can use the function keys as follows:

F1 **Help**	To access the analyzer's help facility (which is not accessible while actively capturing). If capturing in the Expert window, the function key label will read "Explain." You will receive a context-sensitive Explain message if you press F1 in that situation.
F2 **Display active**	To toggle the display between showing either all connections/sessions or only active connections/sessions. Applicable only in Sniffer Internetwork Analyzer (SDLC/SNA, HDLC/X.25, or Frame Relay) views.

F3 **Data display**	To stop the capture and use the Display function. If you press F3, you *cannot* resume the earlier capture (but you can start a new capture, which first clears the capture buffer).
F4 **Clear screen**	To clear the current display on the screen. Frames in the capture buffer are not affected.
F5 **Menus**	To return to the main menu.
F6 **Capture options**	To change the capture options. Frames already in the capture buffer are not affected. If you make any changes to the options or filters, the analyzer clears the screen before resuming capture if you press F6 **[Return]** or F9 **[Resume]**.
F9 **Resume**	To continue the capture. The next frame to be captured is appended to the capture buffer after the last frame captured before you pressed F9. There is no indication to show that a pause occurred.
F10 **New capture**	To start a new capture.

What You Can Do When Capture Has Stopped

Once capture has stopped, you can either display, save, or discard the frames in the capture buffer.

Display	Press F3 **[Data display]** to interpret and display the frames in the capture buffer. For details, see Chapter 7.
Save	You can save the frames in the capture buffer and use the resulting data files as a source for capturing frames. For more information, see "Defining the Capture Source: Live Network or Data File" on page 6–11.
Discard	When you start a new capture or exit from the application without saving the contents of the capture buffer, the Sniffer analyzer displays a warning dialog box (Figure 6–50). If you press ENTER, the frames in the capture buffer are discarded.

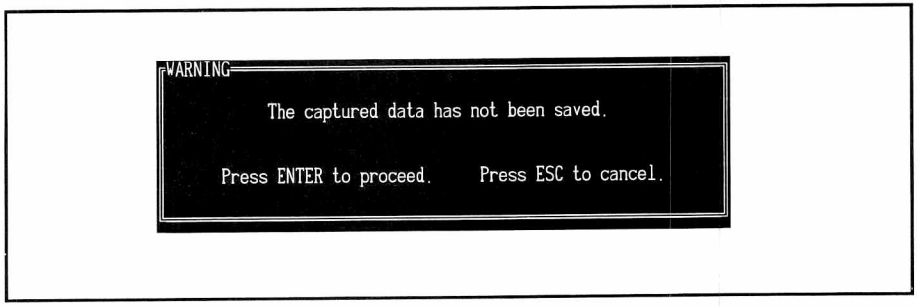


Figure 6–50. Discarding captured frames

Displaying Interpreted Frames

7

Displaying Interpreted Frames

Overview

This chapter describes one of the Sniffer Network Analyzer's central functions: displaying information about the various layers of protocols embedded in the captured frames. It covers these topics:

- Setting filters to limit which frames are displayed
- Displaying frames at three levels of detail, in either the normal or the two-viewport format
- Searching for frames in the displays
- Editing frames in the Hexadecimal display
- Printing and exporting data
- Interpreting protocols

The **Protocol forcing** display option is described in Chapter 9, "Using Protocol Forcing." Protocol forcing is an advanced Sniffer analyzer function that lets you invoke a specific protocol interpreter (PI) for a frame or set of frames.

Display Menu Overview

Figure 7–1 provides an overview of the basic menu items associated with the Display menu. Many of these items, in turn, have associated options. Beneath the menu is a brief explanation of the highlighted option (**Two viewports** in the example). Although the figure shows the menu as it appears for an Ethernet Sniffer Network Analyzer, the basic Display menu items are the same for all networks.

As with other Sniffer analyzer menu options, press the cursor keys to move the highlight to the desired option and then to define that option.

- For options marked with the √ and x symbols, you can press Spacebar to enable (√) or disable (x) the option.
- For options connected with a vertical bar (radio control), you can choose one of those options by moving to it and pressing Spacebar.
- For options where you must define a specific value, such as the range of frames to print, you can either choose that value from a list or enter the desired value into a dialog box.

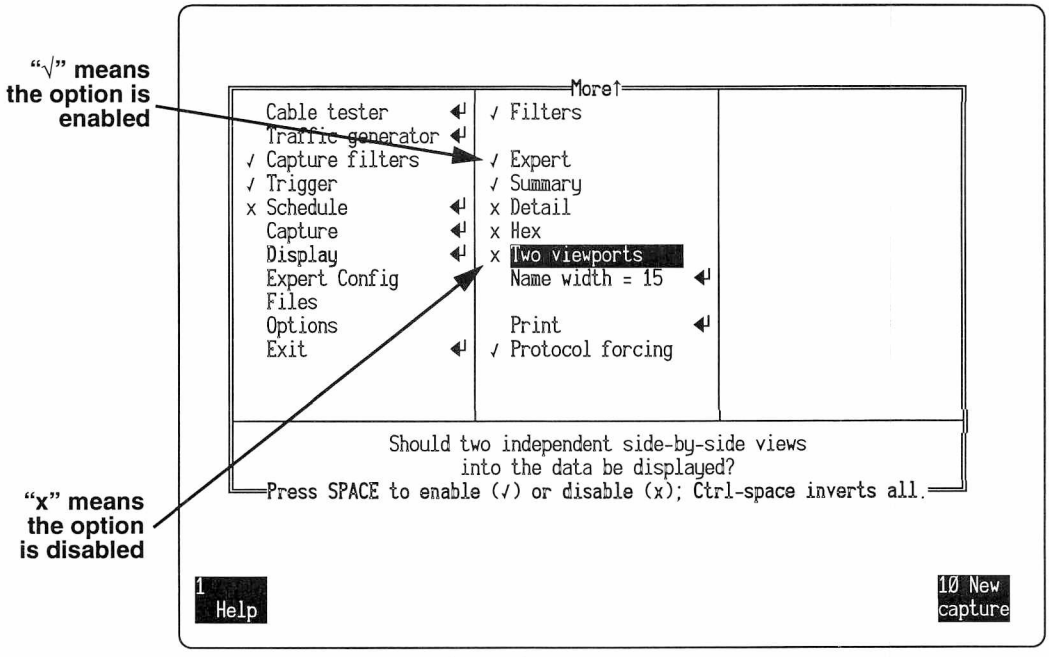


Figure 7–1. Overview of the Display menu options

Role of the Capture Buffer in Displaying Frames

Once the capture buffer contains captured frames, you can interpret those frames and display the results. For an overview of how the analyzer processes frames, see Figure 1–1 on page 1–7.

Frames may be in the capture buffer either as the result of a capture or because they were loaded from a file that was saved during a previous capture session. Whenever you start a new capture session or when you load a file, the frames currently in the buffer are lost. If you try to do so, the Sniffer Network Analyzer displays a warning dialog box that lets you save the frames in the capture buffer as a file.

Setting the Display Filters

As with the capture filters, which limit the frames that are captured, the display filters let you eliminate from display those frames that don't interest you. You can set the display filters either before you display captured frames or while you are displaying them.

Filtering does not remove frames from the capture buffer, it simply excludes them from the display. When frames are excluded, those that are displayed have the same frame numbers as before. For example, you might see frame 30 followed by frame 35 because a display filter excluded frames 31–34. When you save the contents of the capture buffer to a file, you can choose to either save all frames or only those that pass the display filters.

Overview of Available Filters

Figure 7–2 shows the available display filters.

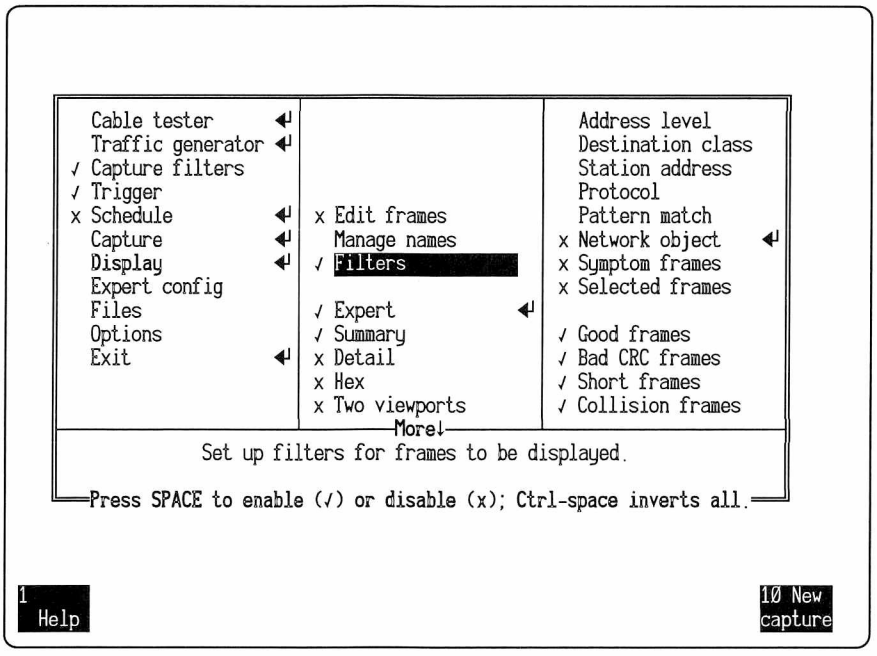


Figure 7–2. The display filters

The following display filters are available for all LANs:

Address level — For frames that contain an address in one of the enabled protocols.

Destination class — For frames that contain a DLC address in the indicated class (broadcast or specific).

Station address — For frames that contain any of up to four specific addresses at any of the levels selected by the **Address level** filter.

Protocol For frames that contain one or more of the enabled protocols.

Pattern match For frames that contain the logical combination of patterns you specify.

Selected frames For frames you flagged with the "S" flag.

If a frame meets the criteria for one filter, the Sniffer analyzer continues to test for the other filters. As a result, a frame may match several of the display filters.

In addition, the following display filters are available for Ethernet, StarLAN, and PC Network:

Good frames For frames that do not contain detected frame defects.

Bad CRC frames For frames with a bad CRC check.

Short frames For frames of less than 60 bytes (runts).

Collision frames (Ethernet-II Sniffer analyzers only) For frames that resulted from collisions.

If a frame meets the criteria for one frame defect the analyzer does not test for any of the others.

The following display filters are available for WAN/Synchronous links:

Address level For frames that contain an address in one of the enabled protocols.

Destination class For frames that contain a DLC address in the indicated class (broadcast or specific).

Station address For frames that contain any of up to four specific addresses at any of the levels selected by the **Address level** filter.

Protocol For frames that contain one or more of the enabled protocols.

Pattern match For frames that contain the logical combination of patterns you specify.

Selected frames For frames you flagged with the "S" flag.

Bad CRC frames For frames with a bad CRC check.

The following filters are available for those networks for which Expert analysis is available (Ethernet, token ring, WAN/Synchronous):

Network object	For frames associated with a specified network object.
Symptom frames	For those frames associated with symptoms.

Each of these filters is explained in more detail after the procedure that follows.

Procedure: Specifying the Display Filters

To set display filters before you start the display:

1. Move to **Display\Filters**. If necessary, press Spacebar to enable (√) the option.
2. Move to the desired filter and press Spacebar to enable (√) or disable (x) that filter.
3. For filters with associated options, define those options.

To change filters (or display options) during the display:

1. Press F6 **[Display options]**. In response, the Sniffer analyzer superimposes the Display Options menu (shown in Figure 7–3) over the display window.

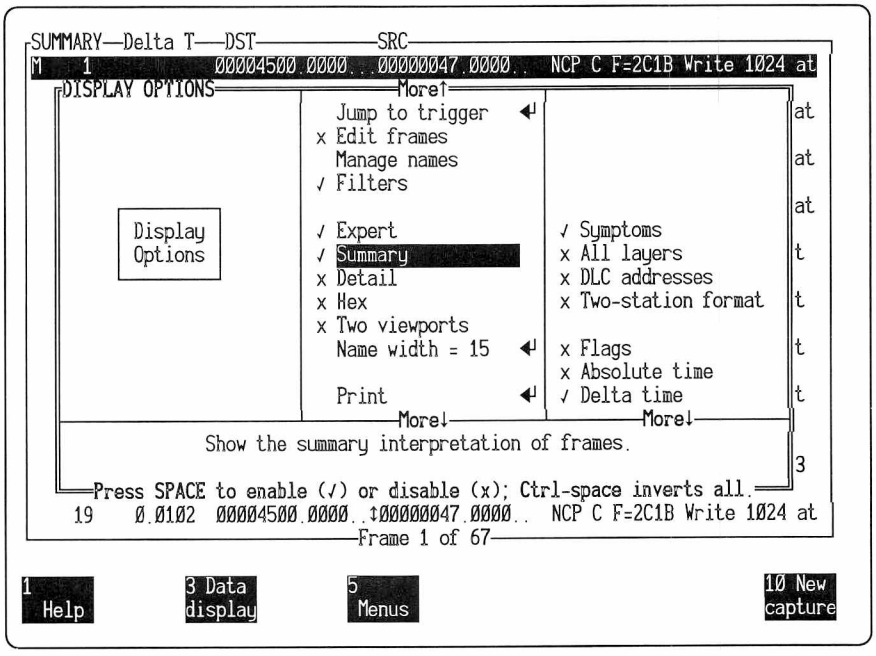


Figure 7–3. The Display Options menu

2. Move to **Filters** and make the desired changes in the filters.
3. Press F3 **[Data display]** to return to the display, which will be modified according to the changes you made.

Address Level Filter

When you set an **Address level** filter, you can enable one or more protocols associated with the **Address level** filter. As a result, the filter accepts only those frames that are addressed in one of the protocols you enabled. Therefore, to be included in the display, a frame must contain both:

- An address level from the enabled set of protocols
- An address in that protocol

Figure 7–4 shows the protocol layers associated with the **Address level** filter. The default is only the lowest protocol layer (DLC) enabled (√). Since every frame has a low-level address, the default accepts all frames.

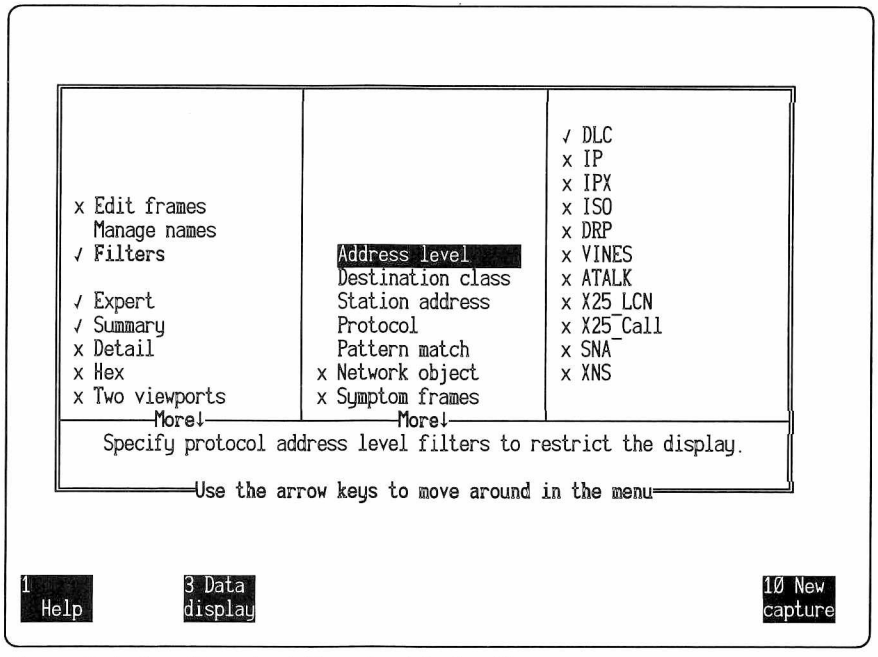


Figure 7–4. Specifying the Address level display filters

Every frame contains both the address of the station from which it just came and the address of the station that is its immediate destination. These addresses are in the frame's lowest level, usually DLC. However, a frame frequently contains other addresses as well. For example, it may contain the address of the original source and the address of the ultimate destination. This means that the data field of a lower-level frame may include a message written in a higher-level protocol, with its own source and destination, written according to that protocol's rules.

This is usually the case for all frames on a WAN/Synchronous communications link. It is also very likely when frames are relayed through a gateway between LANs. At the DLC level, a frame's source and destination may be the stations responsible for the current leg of its journey. Within the DLC frame, there may be addresses in embedded protocols such as XNS, IP, X.400, and so on.

Although many protocols require that the frame include an address, that requirement is not universal. If the protocol permits both addressed and unaddressed messages, an **Address level** filter accepts a frame only when it actually contains an address.

To set an Address level display filter:

1. Move to **Display\Filters\Address level.**

2. Move to the protocols you want to enable (√) or disable (x) and press Spacebar accordingly.

Effect on Displayed Frames

The effect on the displayed frames depends on the display options you choose when defining the Summary view. If you enable the **All layers** option, any enabled protocols are shown, with the highest level on top. Unless you also enable the **DLC addresses** option, the address associated with the highest level protocol is shown. For more information, see "The Summary View Display Options" on page 7–35.

Destination Class Filter

During display, the **Destination class** filter lets you include or exclude messages addressed (at any level) to a broadcast destination[1] or to frames with specific addresses. Of course, if you exclude both options, there is nothing left to look at.

For each destination class you include (broadcast or specific), you can also specify the address level (or levels) to be included, as shown in Figure 7–4. The default is all address levels enabled, so that the **Destination class** filter accepts all frames. The Sniffer Network Analyzer accepts a frame if it includes the desired type of address at *any* of the levels that are enabled.

Figure 7–5 shows the two options associated with the **Destination class** display filter. The default is both options enabled (√).

1. During capture, however, the Sniffer analyzer can filter for broadcast addresses only at the DLC level.

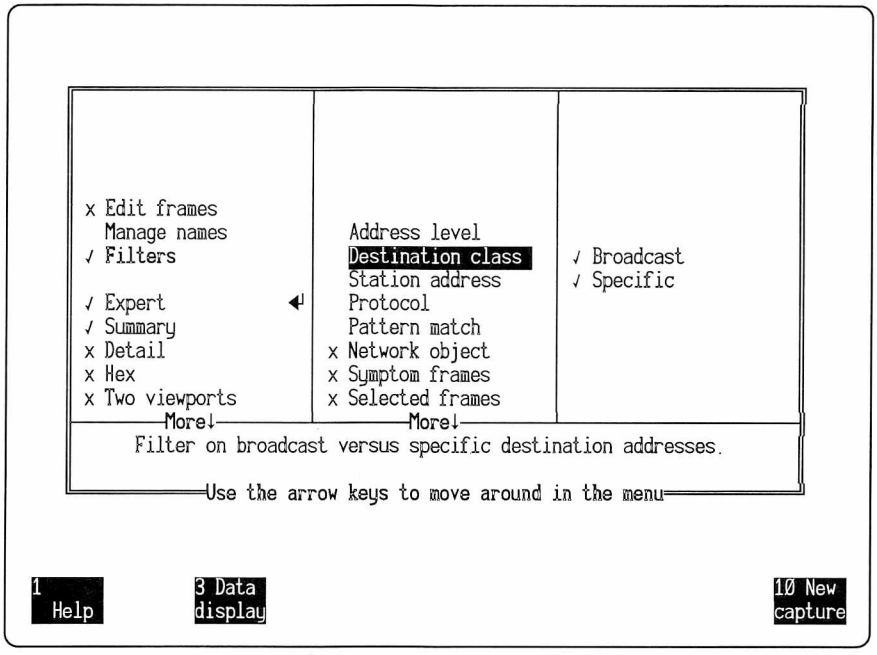


Figure 7–5. Specifying the Destination class display filter

To set a destination class display filter:

1. Move to **Display\Filters\Destination class**.
2. Move to **Broadcast** or **Specific**. Press Spacebar to enable (√) or disable (x) those options.
3. If you enabled the **Broadcast** option, press ENTER and make sure the desired address levels for the **Broadcast** option are enabled or disabled. To enable or disable an address level, move to the desired levels and press Spacebar.
4. Similarly, if you enabled the **Specific** option, make sure the desired address levels for the **Specific** option are enabled or disabled. Note that, although the two lists contain the same address levels, your selections of **Broadcast** addresses are independent of those for **Specific** addresses.

Station Address Display Filter

A **Station address filter** consists of some logical combination of up to four matches, which consist of four pairs of addresses. Address filters for display work just like address filters for capture, but with one important difference. During display, the addresses you

specify can be at any level recognized by the protocol interpreters. By contrast, a capture filter can only filter for low-level addresses.

The procedure for setting an address filter for display is similar to the procedure for setting an address filter for capture, as described in "Defining the Station Address Filters" on page 6–41.

To set a station address filter for display:

1. Move to **Display\Filters\Station address\Match 1.**
2. If you want to name this match, press ENTER. In the dialog box that appears (shown in Figure 7–6), type a name and press ENTER.

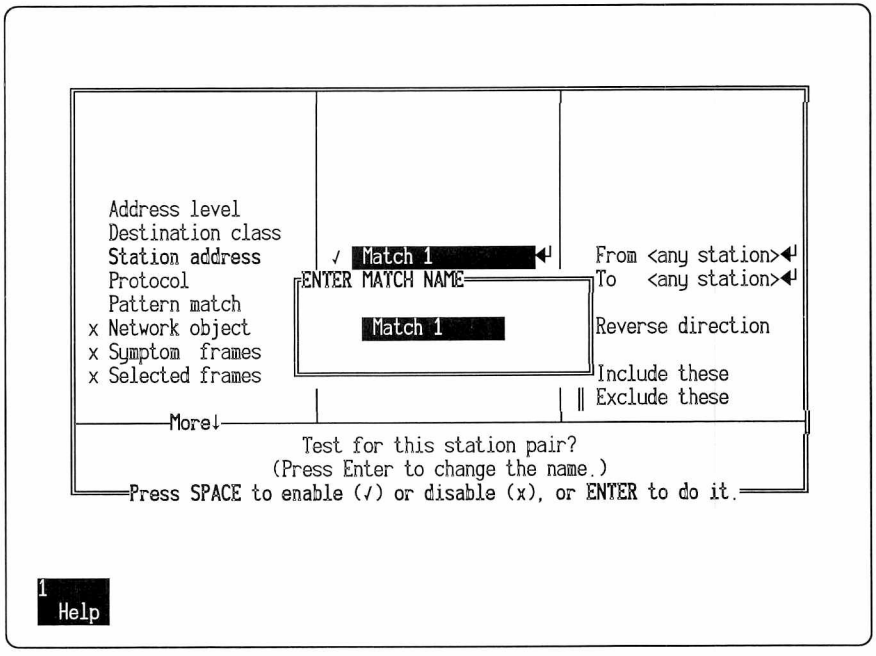


Figure 7–6. Naming a station address filter match

3. To specify a source address, move to **From** and press ENTER. In the table that appears (shown in Figure 7–7), move to the desired station and press ENTER. (If you enabled the **DLC addresses** option in the **Display\Summary** menu, the DLC address is automatically highlighted. If that option is disabled (the default) the highest level address is highlighted.)

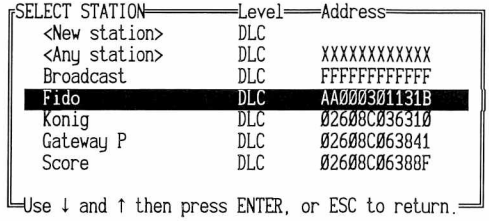


Figure 7–7. Selecting a station as a station address filter

Note that the address—either its name, if it has one, or the numeric address—replaces **<any station>** in the **From** menu item.

4. If the address you want is not in the table, move to the top of the screen, to the **<New station>** item that matches the desired address level and press ENTER. In the dialog box that appears, type a new address and a corresponding name and press ENTER. Figure 7–8 shows the dialog box for entering a new station.

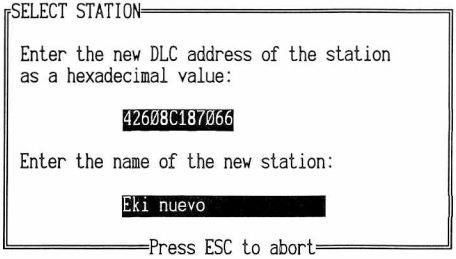

SELECT STATION
Enter the new DLC address of the station
as a hexadecimal value:
42608C187066
Enter the name of the new station:
Eki nuevo
Press ESC to abort

Figure 7–8. Defining a new station as a station address filter

5. To specify a destination address, move to **To** and press ENTER. Repeat the instructions in step 3 for selecting an address. The DLC address is automatically highlighted if you enabled the **DLC addresses** option in the **Display\Summary** menu. Otherwise, the highest level address is highlighted.
6. To specify whether this match also applies to traffic in the reverse direction, move to **Reverse direction** and press Spacebar to enable (√) the option.
7. To specify whether to include or exclude frames identified by this match, move to either **Include these** or **Exclude these** and press Spacebar to select the option you want.

   ▶Include these
   Exclude these
8. Repeat steps 1 through 7 for up to four matches.
9. To specify what to do with frames not covered by the matches, move to **Others** and either to **Include** or **Exclude**. Press Spacebar to specify the desired option.

Considerations when Setting Address Filters

When capturing, address filters are limited to matching DLC addresses. When displaying, address filters allow for higher level addresses as well. However, several considerations apply to both modes:

- Using fewer than four address matches
- Disabling defined address matches
- Taking advantage of the address match order

For additional information about these topics, see "Defining Station Address Matches: Some Considerations" on page 6–40.

Adding Addresses to the Name Table

If the address you want is not in the name table, you must add it to the table before you can select it as an address filter.

To facilitate this process, you can capture traffic that includes the addresses for which you want to filter and then display the results. In response, the Sniffer Network Analyzer adds detected addresses to the top of the name table. You can then name them manually, if you want, to save them permanently. For more information about using the name table, see "Assigning Names to Addresses" on page 8–6.

Protocol Display Filter

In contrast to the **Protocol** capture filter, which filters on the particular SAP or at the DLC level, the **Protocol** display filter can filter for any of the protocols recognized by the protocol interpreters. The default is to accept every protocol.

When you move to the **Protocol** option, the panel to the right displays a list of protocols, shown in Figure 7–9. Note that, because this list includes higher-level protocols, it is much longer than the list associated with the capture filters. Beside each name, a √ indicates that the display filter will display that protocol, an x that it will not. The filter accepts a frame in the display when it contains *any* of the protocols you enable.

NOTE: A special situation occurs for higher-level protocols (for example, SNMP) that use ASN.1 encoding. You can disable the display of these higher level protocols, but if you do not also disable the display of ASN.1, you will still see these protocols mentioned in the frame characterization area at the right of the display. At first, it might appear that the higher-level protocol has not been disabled. However, a closer look will reveal that the higher-level protocol decode is not displayed. It is simply a property of ASN.1 encoding to identify the protocol that is using it.

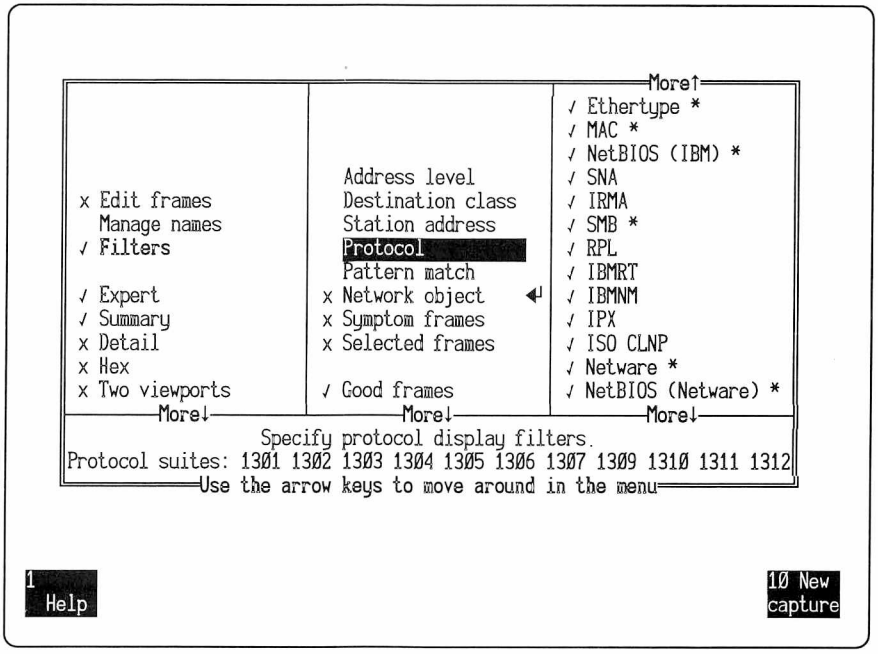


Figure 7–9. Specifying the Protocol display filters

To define the Protocol display filters:

1. Move to **Display\Filters\Protocol**.
2. In the associated list, move to any protocols you want to disable and press Spacebar (x).

To enable only one protocol filter:

By default, all protocols are enabled. You can use the following shortcut to enable just one—or a few—protocols.

1. Press CTRL-Spacebar to disable all protocols (x).
2. Move to the protocol you want to enable and press Spacebar (√).

Pattern Match Display Filter

A pattern is a particular sequence of bits within a frame (specified in hex or binary code, or as ASCII text). In a simple pattern, the bits occur at just one location. In a complex pattern, a set of up to eight simple component patterns is linked with AND/OR logic.

The considerations related to defining a pattern match as a display filter are the same as for defining such a pattern as a capture filter. For complete information on pattern matching, see "Four Contexts for Pattern Matching" on page 6–45.

To set up a pattern match filter for display:

1. Move to **Display\Filters\Pattern match\Match 1.**
2. Follow the procedure "To define a pattern match for a capture filter:" on page 6–53, starting with step 2.

Selected Frames Display Filter

This filter works in conjunction with the "S" flag, which is applied to the highlighted frame during display if you press F9 **[Select frame]**. By enabling the **Selected frames** display filter and disabling all other filters, you can create a file that contains just the frames you flagged and then save those frames as a file.

To filter only for selected frames:

1. In the **Summary** view, move to the frames you want to select and press F9 **[Select frame]**.
2. Move to **Display\Filters\Selected frames** and press Spacebar to enable (√) the option.
3. Disable all other **Display\Filters** options.
4. Press F3 **[Data display]** to display the frames.

To save selected frames to disk:

1. Move to **Files\Save\Data** and press Spacebar to enable (√) the **Filtered only** option.
2. Press ENTER. In the dialog box that appears, name the file that contains the selected frames.

Filters for Defective Frames

On Ethernet, StarLAN, and PC Network Sniffer Network Analyzers, you can filter frames for either the presence or absence of certain defects. This ability is available only if the adapter card retains defective frames and passes them to the analyzer's CPU. On token ring, FDDI, and WAN/Synchronous networks, the adapter card does not pass defective frames to the Sniffer Network Analyzer.

The breakdown for good and defective frames includes:

- Good frames that contain none of the detected defects
- Bad CRC frames, which include frames found to be defective by the CRC
- Short frames, which include frames shorter than 60 byte (runts)
- Collision frames (Ethernet-II only), which indicate collisions

For more information about how defective frames are counted and flagged, see "How the Defective Frames Filters Work (Ethernet)" on page 6–58.

To set filters for good frames or for frame defects:

1. Move to **Display\Filters** and then to the defect category for which you want to filter.
2. Press Spacebar to enable or disable the desired options.
   √ Good frames
   √ Bad CRC frames
   √ Short frames
   √ Collision frames (Ethernet-II only)

Expert Display Filters

This section describes display filters specific to the Expert analyzer. Display filters determine which frames in the capture buffer will be displayed. Eliminating a frame from display with a display filter does not remove the frame from memory. Rather, it simply removes the frame from display. If the display filter eliminating a given frame from display were to be disabled, that frame would reappear.

This section describes the following Expert display filters:

- Network object display filter
- Symptom frames display filter

Network Object Filter

From the Expert window, you can determine what frames to include in the display. For example, you can include in the subsequent display only those frames that are related to a particular diagnosis or that are transmitted on a selected connection. This avoids cluttering up the display with frames that are irrelevant to the problem you want to investigate. The filtering is "automatic" because it does not require you to set up a filter as you normally would with the **Filters** option in the **Display** menu. Instead, you use the function key F2 **[Filter&disply]** to implement the **Network object** filter and determine the frames included for display.

IMPORTANT: The F2 key works as a toggle for setting and removing Network object filters. You cannot set a new **Network object** filter until you have cleared the existing one (unless there is no existing one).

The **Network object** filter does not remove frames from the capture buffer but omits them from the display. When some frames are skipped, the frames that remain visible have the same frame numbers as before. Thus, you may see frame 30 followed by frame 35 because the network object filter excludes frames 31-34.

To set an automatic Network object filter:

1. Display the contents of the capture buffer in the Expert window.
2. The Expert window appears. Display an Expert Summary screen and highlight one of the following:
   - In a Diagnosis Summary screen, a diagnostic message at any layer.
   - In a Symptom and Network Object Summary window, a connection at the Application or Connection layers, or a station at the Network Station or DLC Station layers.

   The function key F2 **[Filter&displ**y] appears at the bottom of the screen. Figure 7–10 shows the Diagnosis Summary screen at the Connection layer.

   If a **Network object** filter is already set, clear the existing filter before setting a new one. (The label for the function key F2 will indicate this by reading **Remove filter** rather than **Filter&displ**y.)
3. Press F2 **[Filter&displ**y].

   In response, the analyzer automatically filters out all frames irrelevant to the highlighted diagnosis, symptom, or network object, and takes you to the Classic window specified in the **Display** menu.

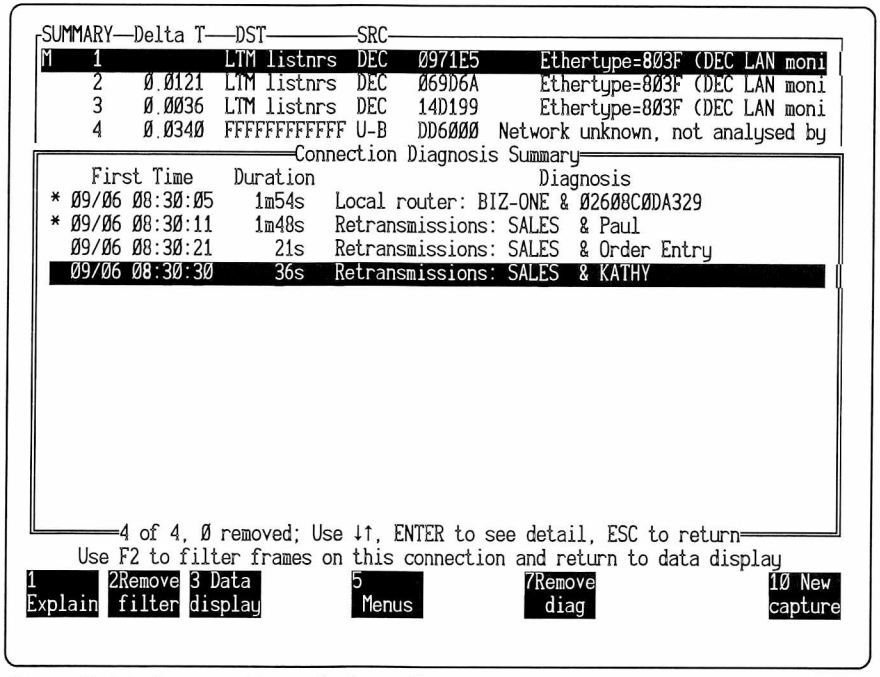

SUMMARY—Delta T—DST——SRC
M 1 LTM listnrs DEC 0971E5 Ethertype=803F (DEC LAN moni
2 0.0121 LTM listnrs DEC 069D6A Ethertype=803F (DEC LAN moni
3 0.0036 LTM listnrs DEC 14D199 Ethertype=803F (DEC LAN moni
4 0.0340 FFFFFFFFFFFF U-B DD6000 Network unknown, not analysed by
Connection Diagnosis Summary
First Time Duration Diagnosis
* 09/06 08:30:05 1m54s Local router: BIZ-ONE & 02608C0DA329
* 09/06 08:30:11 1m48s Retransmissions: SALES & Paul
09/06 08:30:21 21s Retransmissions: SALES & Order Entry
09/06 08:30:30 36s Retransmissions: SALES & KATHY
4 of 4, 0 removed; Use ↓↑, ENTER to see detail, ESC to return
Use F2 to filter frames on this connection and return to data display
1 Explain
2Remove filter
3 Data display
5 Menus
7Remove diag
10 New capture

Figure 7–10. Setting a Network object filter

Example: Setting a Network Object Filter

For example, in Figure 7–10 the analyzer has diagnosed four problems at the Connection layer. If you want to focus on the frames that are relevant to the highlighted diagnosis ("Retransmissions between SALES and Kathy"), highlight the diagnostic message. Press F2 **[Filter&displ]** to display only those frames relevant to the highlighted diagnosis. The subsequent display is shown in Figure 7–11. Notice that the display starts with frame 448 and that the frame numbers are not contiguous. The displayed frames are the ones that lead to the diagnosis, "Retransmissions between SALES and Kathy."

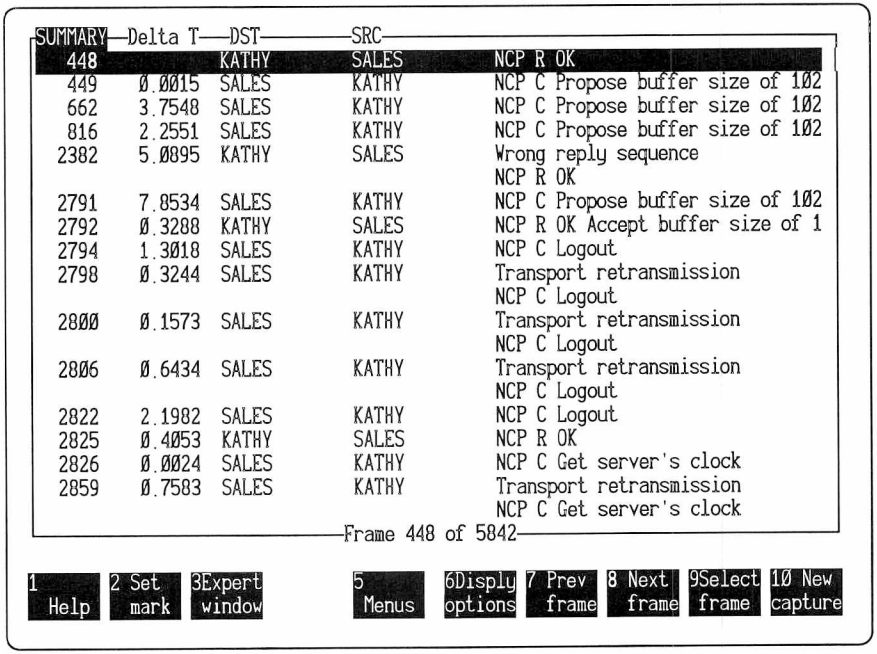

SUMMARY Delta T DST SRC
448 KATHY SALES NCP R OK
449 Ø.ØØ15 SALES KATHY NCP C Propose buffer size of 1Ø2
662 3.7548 SALES KATHY NCP C Propose buffer size of 1Ø2
816 2.2551 SALES KATHY NCP C Propose buffer size of 1Ø2
2382 5.Ø895 KATHY SALES Wrong reply sequence
NCP R OK
2791 7.8534 SALES KATHY NCP C Propose buffer size of 1Ø2
2792 Ø.3288 KATHY SALES NCP R OK Accept buffer size of 1
2794 1.3Ø18 SALES KATHY NCP C Logout
2798 Ø.3244 SALES KATHY Transport retransmission
NCP C Logout
28ØØ Ø.1573 SALES KATHY Transport retransmission
NCP C Logout
28Ø6 Ø.6434 SALES KATHY Transport retransmission
NCP C Logout
2822 2.1982 SALES KATHY NCP C Logout
2825 Ø.4Ø53 KATHY SALES NCP R OK
2826 Ø.ØØ24 SALES KATHY NCP C Get server's clock
2859 Ø.7583 SALES KATHY Transport retransmission
NCP C Get server's clock
Frame 448 of 5842
1 Help
2 Set mark
3Expert window
5 Menus
6Disply options
7 Prev frame
8 Next frame
9Select frame
1Ø New capture

Figure 7–11. Summary display with Network object filter set on the diagnosis "Retransmissions between SALES and Kathy"

The **Network object** filter lets you zero in on a particular diagnosis or symptom. However, you can also filter frames on any network object that interests you, whether or not the object has associated symptoms. For example, you can display the Network Stations Summary screen, as shown in Figure 7–12. To see all the frames to and from the server "BIZ-ONE," highlight the server's name and press F2 **[Filter&disply]**. The Classic window shown in Figure 7–13 appears, containing all the frames to and from BIZ-ONE on its two connections.

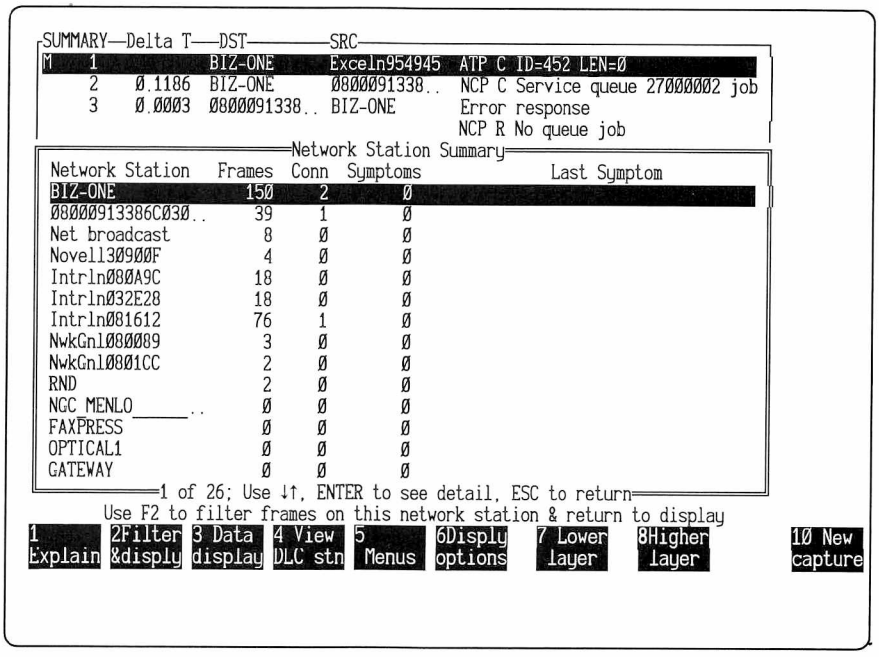

SUMMARY—Delta T—DST—SRC
M 1 BIZ-ONE Exceln954945 ATP C ID=452 LEN=Ø
2 Ø.1186 BIZ-ONE Ø8ØØØ91338.. NCP C Service queue 27ØØØØØ2 job
3 Ø.ØØØ3 Ø8ØØØ91338.. BIZ-ONE Error response
NCP R No queue job
Network Station Summary
Network Station Frames Conn Symptoms Last Symptom
BIZ-ONE 150 2 Ø
Ø8ØØØ913386CØ3Ø.. 39 1 Ø
Net broadcast 8 Ø Ø
Novell3Ø9ØØF 4 Ø Ø
IntrlnØ8ØA9C 18 Ø Ø
IntrlnØ32E28 18 Ø Ø
IntrlnØ81612 76 1 Ø
NwkGnlØ8ØØ89 3 Ø Ø
NwkGnlØ8Ø1CC 2 Ø Ø
RND 2 Ø Ø
NGC MENLO_____.. Ø Ø Ø
FAXPRESS Ø Ø Ø
OPTICAL1 Ø Ø Ø
GATEWAY Ø Ø Ø
1 of 26; Use ↓↑, ENTER to see detail, ESC to return
Use F2 to filter frames on this network station & return to display
1 Explain
2Filter &disply
3 Data display
4 View DLC stn
5 Menus
6Disply options
7 Lower layer
8Higher layer
1Ø New capture

Figure 7–12. Network Stations Summary window

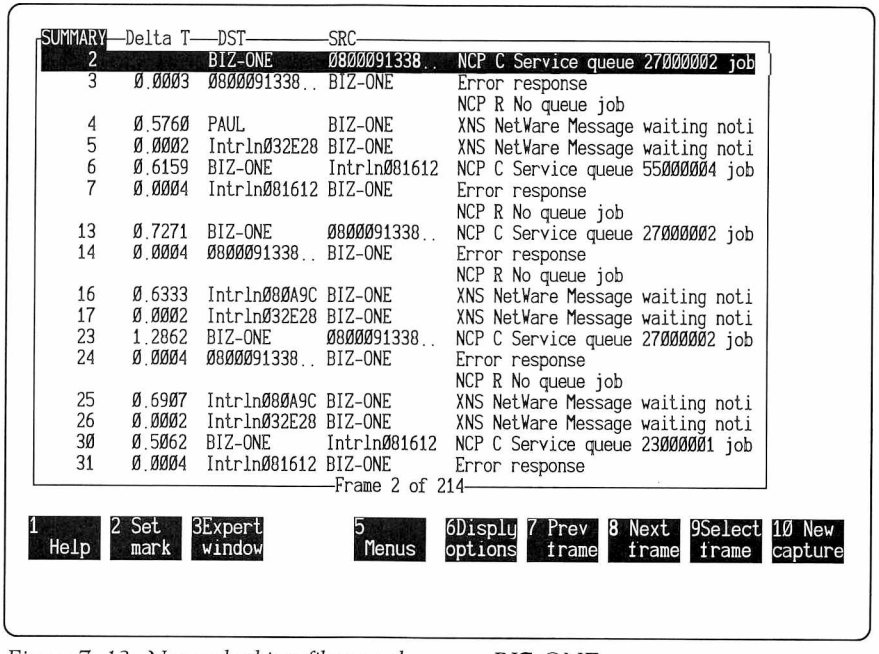

SUMMARY—Delta T—DST—SRC
2 BIZ-ONE Ø8ØØØ91338.. NCP C Service queue 27ØØØØØ2 job
3 Ø.ØØØ3 Ø8ØØØ91338.. BIZ-ONE Error response
NCP R No queue job
4 Ø.576Ø PAUL BIZ-ONE XNS NetWare Message waiting noti
5 Ø.ØØØ2 IntrlnØ32E28 BIZ-ONE XNS NetWare Message waiting noti
6 Ø.6159 BIZ-ONE IntrlnØ81612 NCP C Service queue 55ØØØØØ4 job
7 Ø.ØØØ4 IntrlnØ81612 BIZ-ONE Error response
NCP R No queue job
13 Ø.7271 BIZ-ONE Ø8ØØØ91338.. NCP C Service queue 27ØØØØØ2 job
14 Ø.ØØØ4 Ø8ØØØ91338.. BIZ-ONE Error response
NCP R No queue job
16 Ø.6333 IntrlnØ8ØA9C BIZ-ONE XNS NetWare Message waiting noti
17 Ø.ØØØ2 IntrlnØ32E28 BIZ-ONE XNS NetWare Message waiting noti
23 1.2862 BIZ-ONE Ø8ØØØ91338.. NCP C Service queue 27ØØØØØ2 job
24 Ø.ØØØ4 Ø8ØØØ91338.. BIZ-ONE Error response
NCP R No queue job
25 Ø.69Ø7 IntrlnØ8ØA9C BIZ-ONE XNS NetWare Message waiting noti
26 Ø.ØØØ2 IntrlnØ32E28 BIZ-ONE XNS NetWare Message waiting noti
3Ø Ø.5Ø62 BIZ-ONE IntrlnØ81612 NCP C Service queue 23ØØØØØ1 job
31 Ø.ØØØ4 IntrlnØ81612 BIZ-ONE Error response
Frame 2 of 214
1 Help
2 Set mark
3Expert window
5 Menus
6Disply options
7 Prev frame
8 Next frame
9Select frame
1Ø New capture

Figure 7–13. Network object filter on the server BIZ-ONE

Limitations of the Network Object Filter

The **Network object** filter has two limitations, listed below:

- Some symptoms and diagnoses, such as Broadcast storm, have no associated network object on which the analyzer can filter. In those cases, the F2 function key label will not appear at the bottom of display, indicating that a **Network object** filter cannot be set.
- Occasionally you may set a **Network object** filter on an object that no longer has associated frames in the capture buffer. In that case, you will see the message "`No frames are eligible for display`".

For example, the analyzer may detect a connection between Agnes and the server BIZ-ONE at the beginning of a capture session. After capture has proceeded for several hours, capture is paused, and a **Network object** filter is set on that connection. While the analyzer knows that connection took place, the actual transmitted frames have been pushed out of the capture buffer by newer data. To ensure that the data you are interested in remains in the capture buffer, use a capture filter, or a trigger.

NOTE: The "`No frames are eligible for display`" message can also appear when the highlighted object has never actually sent or received a frame. For example, in the Network Stations Summary screen in Figure 7–12, if you highlight OPTICAL1, pressing F2 **[Filter&disply]** does not cause any filtering because OPTICAL1 has neither sent nor received frames.

Other Notes About the Network Object Filter

The Expert analyzer uses several algorithms to decide which frames are associated with the network object chosen as a filter. Sometimes, these algorithms may eliminate frames you consider relevant. For example, if you set a network object filter on a Novell Netware connection layer connection, the Expert analyzer would show all those related frames with NCP layers, but possibly would eliminate from display some connection maintenance frames that it considers irrelevant.

When you set a filter on a connection object, the frame that initiates the connection will not be included among the frames displayed. This is because Expert does not create a connection object until the connection is completed. Similarly, when you filter on an application object, TCP continuation frames will not be included.

Displaying the Network Object Filter

The Expert analyzer lets you view the network object on which it is filtering.

To display the current Network object filter:

1. Move to **Display\Filters**.
   The display in Figure 7–14 appears.

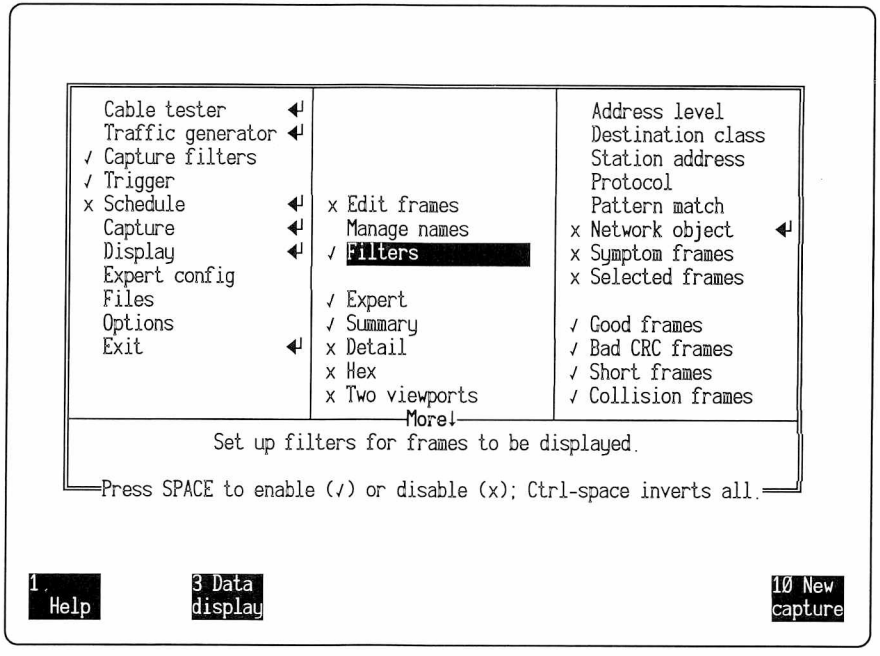


Figure 7–14. The Display\Filters menu

2. Move to **Network object** and press ENTER.

   The analyzer displays the object on which the analyzer is currently filtering. Figure 7–15 shows a **Network object** filter on the connection between the two network stations, SALES and Kathy. Only frames associated with this connection will be displayed under the current **Network object** filter.

NOTE: If no **Network object** filter is currently set, the analyzer will display the message:

```
No Network object filter has been set.
Go to the Expert window to set a filter.
```

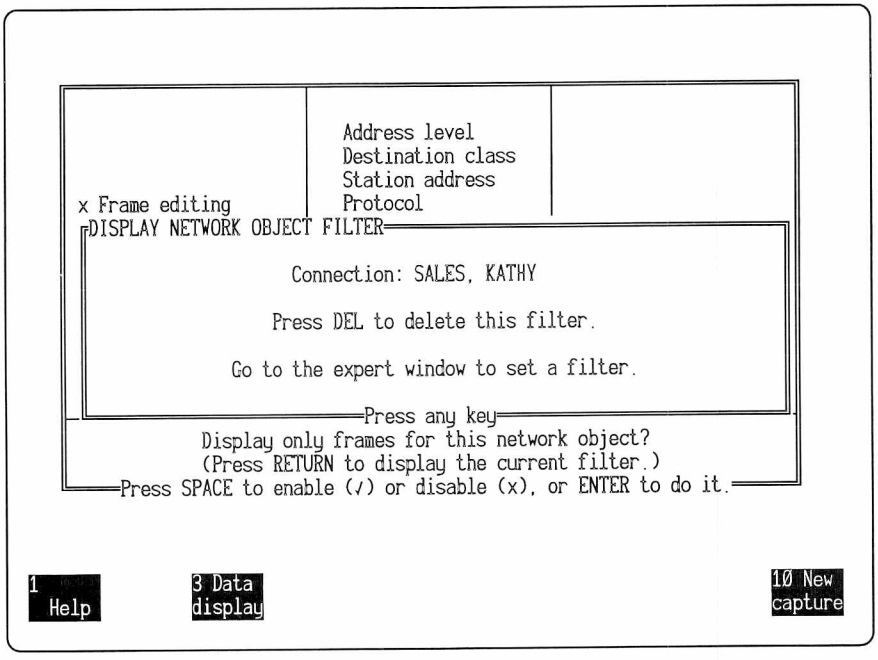

Address level
Destination class
Station address
x Frame editing
Protocol
DISPLAY NETWORK OBJECT FILTER
Connection: SALES, KATHY
Press DEL to delete this filter.
Go to the expert window to set a filter.
Press any key
Display only frames for this network object?
(Press RETURN to display the current filter.)
Press SPACE to enable (√) or disable (x), or ENTER to do it.
1 Help
3 Data display
10 New capture

Figure 7–15. Displaying the current Network object filter

Removing the Network Object Filter

Existing **Network object** filters must be removed before you can set a new one. **Network object** filters can be removed in two ways:

- Using the F2 **[Remove Filter]** function key. The function key F2 acts as a toggle for setting and removing **Network object** filters.
- Using the **Network object** filter menu item in the Display/Filters menu.

For information on setting a new filter, see "To set an automatic Network object filter:" on page 7–18.

To remove a Network object filter using the Network object menu item:

1. Move to **Display\Filters\Network object** and press ENTER.
   The display in Figure 7–15 appears.
2. Press the DELETE key to remove the current **Network object** filter.

Symptom Frames Filter

In addition to the **Network object** display filter, the Expert analyzer also provides a **Symptom frames** display filter. The **Symptom frames** display filter allows you to filter

from display those frames that do not exhibit symptoms. In this way you can filter a huge capture buffer down to just those frames that interest you.

To filter out frames that do not exhibit symptoms:

1. Move to **Display\Filters\Symptom frames.**

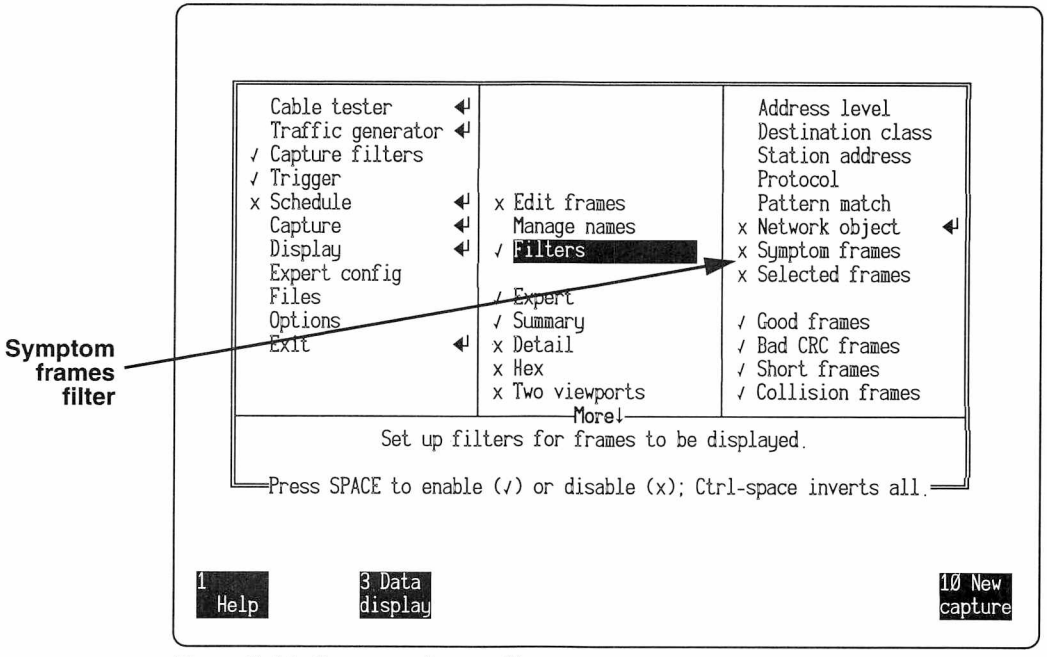


*Figure 7–16. **Symptom frames** filter*

2. Press Spacebar to change the x in front of **Symptom frames** to a √, to enable the **Symptom frames** filter.
3. Press F3 **[Data display]** to display only those frames that exhibit symptoms. Figure 7–17 shows the Summary window with the **Symptom frames** filter enabled.

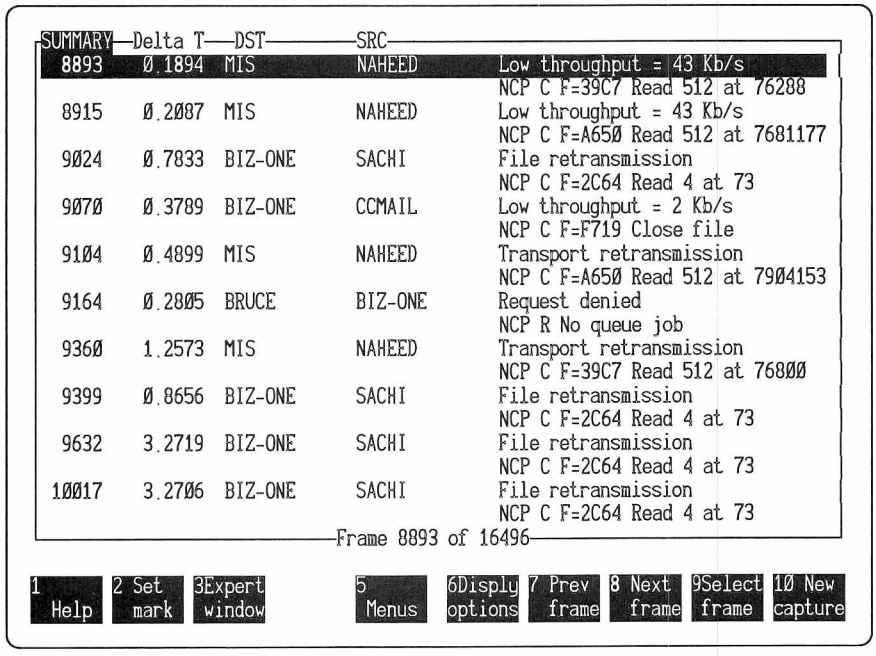

SUMMARY Delta T DST SRC
8893 Ø.1894 MIS NAHEED Low throughput = 43 Kb/s
NCP C F=39C7 Read 512 at 76288
8915 Ø.2Ø87 MIS NAHEED Low throughput = 43 Kb/s
NCP C F=A65Ø Read 512 at 7681177
9Ø24 Ø.7833 BIZ-ONE SACHI File retransmission
NCP C F=2C64 Read 4 at 73
9Ø7Ø Ø.3789 BIZ-ONE CCMAIL Low throughput = 2 Kb/s
NCP C F=F719 Close file
91Ø4 Ø.4899 MIS NAHEED Transport retransmission
NCP C F=A65Ø Read 512 at 7904153
9164 Ø.28Ø5 BRUCE BIZ-ONE Request denied
NCP R No queue job
936Ø 1.2573 MIS NAHEED Transport retransmission
NCP C F=39C7 Read 512 at 768ØØ
9399 Ø.8656 BIZ-ONE SACHI File retransmission
NCP C F=2C64 Read 4 at 73
9632 3.2719 BIZ-ONE SACHI File retransmission
NCP C F=2C64 Read 4 at 73
1ØØ17 3.27Ø6 BIZ-ONE SACHI File retransmission
NCP C F=2C64 Read 4 at 73
Frame 8893 of 16496
1 Help
2 Set mark
3Expert window
5 Menus
6Disply options
7 Prev frame
8 Next frame
9Select frame
1Ø New capture

Figure 7–17. Classic Summary display with ***Symptom frames*** *filter enabled*

Disabling the Display Filters

If you find that the frames that interest you are not displayed, you might suspect that a display filter is eliminating those frames. By temporarily disabling the display filters, you can seee whether the display filters are removing the frames that interest you from the display.

There are two ways to disable the display filters you selected:

- Disabling the **Display\Filters** option
- Using the **Use defaults** option

By disabling the **Display filters** option, you *temporarily* disable all display filters. This allows you to display all the frames in the capture buffer to make sure the frames of interest were captured, without having to disable individual filters you may have spent considerable time setting up. After examining the display without the filters, you can fine-tune your display filters.

To disable all selected display filters temporarily:

1. Move to **Display\Filters** and press Spacebar to disable (x) the option.

If you choose the **Use defaults** option, all selected display filters *and* all other options are reset to the factory default settings. Because you may have spent considerable time defining various options, *do not* use the **Use defaults** option unless you want to start over again, using the factory defaults.

NOTE: You can also use the **Files\Save\Setups** option to save the current configuration of options (including the display filters) to a file and then apply those options to other captures.

Displaying Interpreted Frames

After frames are captured and stored in the capture buffer, you can use the **Display** command to start the interpretation. Those frames that pass the display filters are processed by the protocol interpreters, which decode the various protocol layers embedded in each frame. Although the lowest-level protocols are interpreted automatically depending on your network, separate protocol interpreter suites interpret higher-level protocols by first dissecting each frame into its component layers and then decoding each layer according to its protocol.

The Display Options: An Overview

Depending on which display options you enable, you can show the results of the interpretation in one or more of the following views:

- **Expert** view, which shows network objects, symptoms, and diagnoses identified by the Expert analyzer.
- **Summary** view, which shows either a one-line summary of each frame or several lines, with one for each enabled protocol level within a frame.
- **Detail** view, which shows the contents of the interpreted protocols within the frame, including the fields and parameters within each protocol. Since a low-level frame may contain higher-level frames, a single frame may require several levels of interpretation.
- **Hexadecimal** view, which shows all bytes within the frame to provide a record of the received data. Depending on the network, you can choose either an ASCII or EBCDIC interpretation, or let the Sniffer analyzer adjust the interpretation automatically.

You can view the results of the interpretation of frames in the Summary, Detail, and Hexadecimal views, either individually or simultaneously. When you display more than one view, the Summary view is on top, the Detail view is in the middle, and the Hex view is at the bottom, as shown in Figure 7–18.

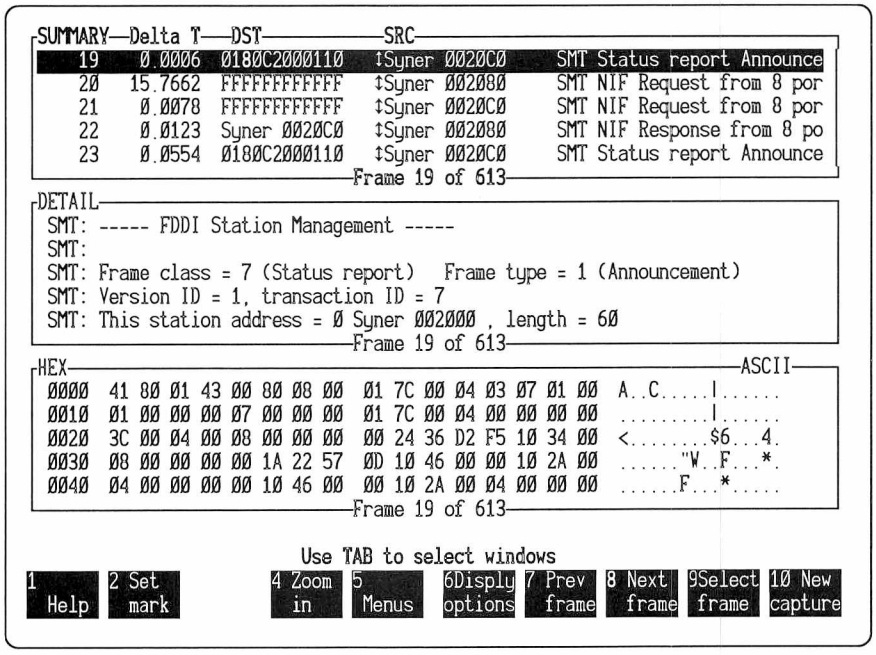

SUMMARY—Delta T—DST—SRC
19 Ø.ØØØ6 Ø18ØC2ØØØ11Ø ‡Syner ØØ2ØC0 SMT Status report Announce
2Ø 15.7662 FFFFFFFFFFFF ‡Syner ØØ2Ø8Ø SMT NIF Request from 8 por
21 Ø.Ø078 FFFFFFFFFFFF ‡Syner ØØ2ØC0 SMT NIF Request from 8 por
22 Ø.Ø123 Syner ØØ2ØC0 ‡Syner ØØ2Ø8Ø SMT NIF Response from 8 po
23 Ø.Ø554 Ø18ØC2ØØØ11Ø ‡Syner ØØ2ØC0 SMT Status report Announce
Frame 19 of 613
DETAIL
SMT: ----- FDDI Station Management -----
SMT:
SMT: Frame class = 7 (Status report) Frame type = 1 (Announcement)
SMT: Version ID = 1, transaction ID = 7
SMT: This station address = Ø Syner ØØ2ØØØ , length = 6Ø
Frame 19 of 613
HEX ASCII
ØØØØ 41 8Ø Ø1 43 ØØ 8Ø Ø8 ØØ Ø1 7C ØØ Ø4 Ø3 Ø7 Ø1 ØØ A..C.....|.....
ØØ1Ø Ø1 ØØ ØØ ØØ Ø7 ØØ ØØ ØØ Ø1 7C ØØ Ø4 ØØ ØØ ØØ ØØ .....|.....
ØØ2Ø 3C ØØ Ø4 ØØ Ø8 ØØ ØØ ØØ ØØ 24 36 D2 F5 1Ø 34 ØØ <.....$6...4.
ØØ3Ø Ø8 ØØ ØØ ØØ ØØ 1A 22 57 ØD 1Ø 46 ØØ ØØ 1Ø 2A ØØ .....W..F...*.
ØØ4Ø Ø4 ØØ ØØ ØØ ØØ 1Ø 46 ØØ ØØ 1Ø 2A ØØ Ø4 ØØ ØØ ØØ .....F...*.....
Frame 19 of 613
Use TAB to select windows
1 Help
2 Set mark
4 Zoom in
5 Menus
6Disply options
7 Prev frame
8 Next frame
9Select frame
1Ø New capture

Figure 7–18. Displaying interpreted frames in all three views

In general, all displayed views focus on a single frame. However, by using the **Two viewports** option, you can also look at two different frames simultaneously, in up to six different views (Figure 7–19).

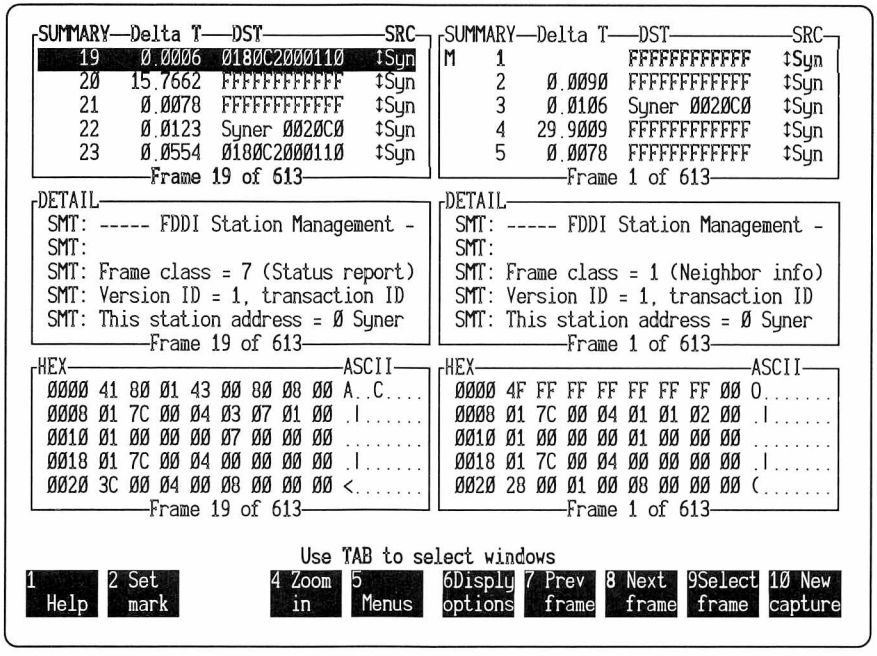

SUMMARY—Delta T—DST—SRC
19 Ø.ØØØ6 Ø18ØC2ØØØ11Ø ↕Syn
2Ø 15.7662 FFFFFFFFFFFF ↕Syn
21 Ø.ØØ78 FFFFFFFFFFFF ↕Syn
22 Ø.Ø123 Syner ØØ2ØCØ ↕Syn
23 Ø.Ø554 Ø18ØC2ØØØ11Ø ↕Syn
Frame 19 of 613
DETAIL
SMT: ----- FDDI Station Management -
SMT:
SMT: Frame class = 7 (Status report)
SMT: Version ID = 1, transaction ID
SMT: This station address = Ø Syner
Frame 19 of 613
HEX—ASCII
ØØØØ 41 8Ø Ø1 43 ØØ 8Ø Ø8 ØØ A..C....
ØØØ8 Ø1 7C ØØ Ø4 Ø3 Ø7 Ø1 ØØ .|......
ØØ1Ø Ø1 ØØ ØØ ØØ Ø7 ØØ ØØ ØØ ....
ØØ18 Ø1 7C ØØ Ø4 ØØ ØØ ØØ ØØ .|......
ØØ2Ø 3C ØØ Ø4 ØØ Ø8 ØØ ØØ ØØ <.......
Frame 19 of 613
SUMMARY—Delta T—DST—SRC
M 1 FFFFFFFFFFFF ↕Syn
2 Ø.ØØ9Ø FFFFFFFFFFFF ↕Syn
3 Ø.Ø1Ø6 Syner ØØ2ØCØ ↕Syn
4 29.9ØØ9 FFFFFFFFFFFF ↕Syn
5 Ø.ØØ78 FFFFFFFFFFFF ↕Syn
Frame 1 of 613
DETAIL
SMT: ----- FDDI Station Management -
SMT:
SMT: Frame class = 1 (Neighbor info)
SMT: Version ID = 1, transaction ID
SMT: This station address = Ø Syner
Frame 1 of 613
HEX—ASCII
ØØØØ 4F FF FF FF FF FF FF ØØ O.......
ØØØ8 Ø1 7C ØØ Ø4 Ø1 Ø1 Ø2 ØØ .|......
ØØ1Ø Ø1 ØØ ØØ ØØ Ø1 ØØ ØØ ØØ ....
ØØ18 Ø1 7C ØØ Ø4 ØØ ØØ ØØ ØØ .|......
ØØ2Ø 28 ØØ Ø1 ØØ Ø8 ØØ ØØ ØØ (.......
Frame 1 of 613
Use TAB to select windows
1 Help
2 Set mark
4 Zoom in
5 Menus
6Disply options
7 Prev frame
8 Next frame
9Select frame
1Ø New capture

Figure 7–19. Displaying interpreted frames with the Two viewports option

What is displayed in the Summary and Hex views depends on the display options you select for those views, described later in "The Summary View Display Options" on page 7–35 and "The Hexadecimal View Display Options" on page 7–51. The Detail view always shows all known information for the current frame.

About the Use of Color

If you have a color monitor, each protocol layer is shown in a different color. Where possible, each layer is identified with one of the seven layers of the OSI model. However, because many protocols predate the OSI model, they may not neatly fit into this scheme.

Normal color displays use a blue background. Highlighted areas are identified by a light-blue background in the Summary and Detail views and a white background in the Hex view.

Figure 7-20 shows the colors associated with various network layers.

Protocol	Layer	Color
Physical level protocols	1	Magenta
Fragmentation protocols	1+	Red
Link level protocols	2	Brown
Network level protocols	3	Green
Transport level protocols	4	Yellow
Session level protocols	5	Light green
Presentation level protocols	6	Light cyan
Application level protocols	7-	Light red
Application level protocols II	7	Light magenta
Name protocols and network management layers		Cyan (blue-green)
Various protocol glue layers		Black
Other (SMT)		Light blue

Figure 7–20. Colors associated with protocol layers

Scrolling within the Display Views

Information that is not visible on the screen can be reached by scrolling. For faster techniques, see "Searching for Frames" on page 7–55.

If you scroll to a frame within one view, all other displayed views also scroll to that frame automatically (see Figure 7–21). For example, if you scroll to highlight a particular frame in the Summary view, the first line pertaining to that frame is highlighted in the Detail view and the corresponding bytes are highlighted in the Hex view. In this way, it is easy to match a sequence of bytes with its interpretation.

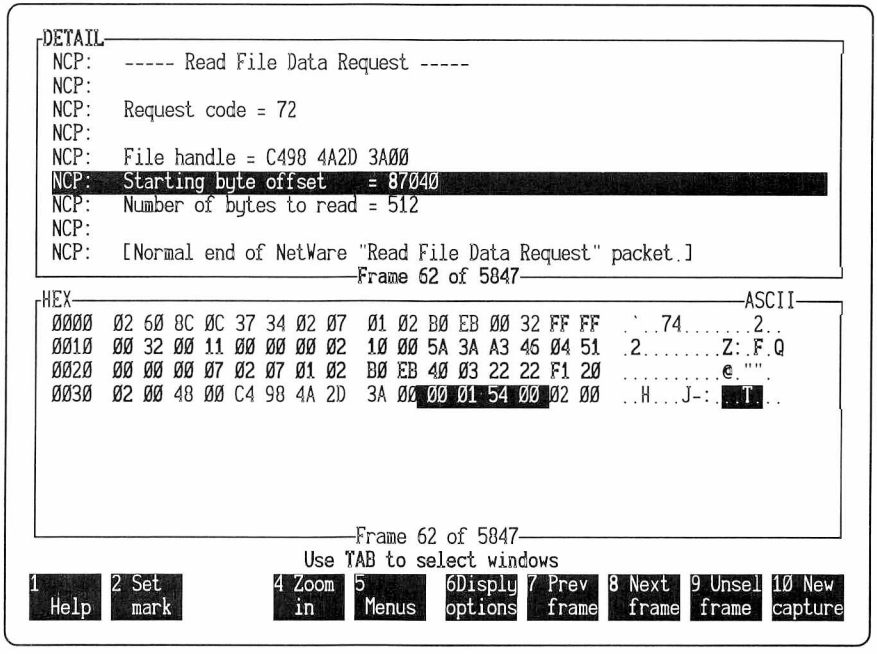

DETAIL
NCP: ----- Read File Data Request -----
NCP:
NCP: Request code = 72
NCP:
NCP: File handle = C498 4A2D 3A00
NCP: Starting byte offset = 87040
NCP: Number of bytes to read = 512
NCP:
NCP: [Normal end of NetWare "Read File Data Request" packet.]
Frame 62 of 5847
HEX
ASCII
0000 02 60 8C 0C 37 34 02 07 01 02 B0 EB 00 32 FF FF .`..74.....2..
0010 00 32 00 11 00 00 00 02 10 00 5A 3A A3 46 04 51 .2.....Z:.F.Q
0020 00 00 00 07 02 07 01 02 B0 EB 40 03 22 22 F1 20 .....@."". .
0030 02 00 48 00 C4 98 4A 2D 3A 00 00 01 54 00 02 00 ..H...J-:...T...
Frame 62 of 5847
Use TAB to select windows
1 Help
2 Set mark
4 Zoom in
5 Menus
6Disply options
7 Prev frame
8 Next frame
9 Unsel frame
10 New capture

Figure 7–21. Synchronized scrolling in the display views

If you enabled the **Two viewports** display option, which splits the screen into two independent viewports, you can scroll independently in each of the two viewports. Within each viewport, however, scrolling in one view automatically scrolls to the corresponding information in the other views.

NOTE: On an FDDI Sniffer Network Analyzer, performance delays may occur when scrolling through a large (up to 32 Mbyte) capture buffer with a display filter set. For example, you display an 18 Mbyte trace file in Summary, Detail, and Hex windows. You then set a protocol filter to look at SMT frames. If you are at the end of the buffer and press F7 **[Prev Frame]**, a delay may occur while the analyzer filters through the large trace file for an SMT frame.

Moving between the Display Views

The view that contains the cursor is said to be *active*. This view is identified by a highlighted border (on a color monitor) or a contrasting color (on a monochrome monitor).

When all three views are open, the Summary view is active when you first press F3 **[Data display]**. To make another view active, press TAB. To move in the reverse direction, press SHIFT-TAB.

Enlarging a Display View

To enlarge the active view and obscure the others, press F4 **[Zoom in]**. To return to the display of all views at the normal size, press F4 **[Zoom out]** again.

Compensation for Bit-Reversal in PC Network Addresses

The Sniffer Network Analyzer for PC Network includes a capture option called **Flip DLC address**. This option changes the way in which bits within each byte of a DLC address are interpreted as characters, which, in turn, changes the address that is visible during display.

During transmission, PC Network follows the low-order-bit-first convention (like Ethernet). However, PC Network often runs software developed for token ring networks. In the computer, IBM software keeps a single representation of station addresses and uses it for both token ring and PC Network operations. This permits the software to keep just one table of DLC addresses, rather than one version for token ring and a separate version for PC Network. To permit a single address table to work despite different conventions for transmission, IBM software for PC Network reverses the bits within each of the 12 bytes that contain the DLC source and destination addresses. In this way, the transmission on the PC Network wire continues to match the IEEE assignment, and the computers linked by PC Network can use the same address tables as those linked by token ring.

To allow PC Network DLC addresses to match those of token ring, enabling the **Flip DLC address** option reverses the order of bits in the frame's source and destination address during capture, before the frame reaches the capture buffer. Thus, the value displayed depends on whether this option was enabled or disabled during capture. Note that the apparent difference in the DLC addresses affects the Summary, Detail, and Hex views.

Once you set the Sniffer Network Analyzer to match a particular network, you do not need to change it further.

Compensation for Bit-Reversal in FDDI Networks

The Sniffer analyzer for FDDI networks includes **Show SMT addresses** and **Show LLC addresses** display options. These options change the way DLC addresses are displayed. in both the Summary and Detail views.

Activating the **Show SMT addresses** option displays all frame addresses in the canonical format rather than using the most significant bit (MSB) form to represent the 48-bit addresses. Using the **Show LLC addresses** displays all frame addresses in the MSB form.

The Summary View

The Summary view provides a condensed view of the captured frames (Figure 7–22). It is the only view that can show several frames at once. Each frame is reduced to a single line or a few lines (depending on whether the **Summary \ All layers** is enabled). Although each frame is abbreviated and condensed, you can see the sequence and context of the frames at a glance. You can then examine individual frames in greater detail or skip over them.

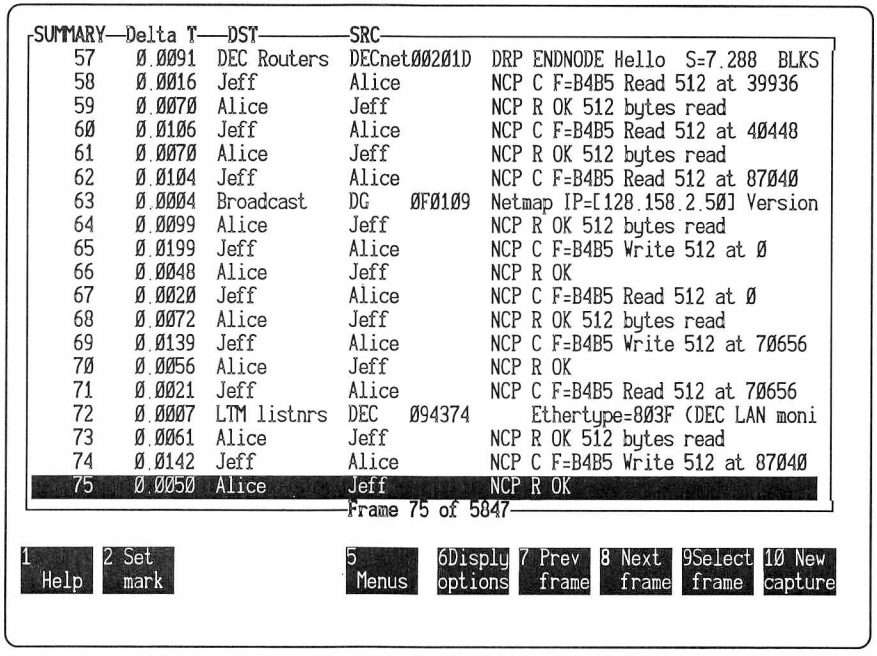

SUMMARY—Delta T—DST——SRC
57 Ø.ØØ91 DEC Routers DECnetØØ2Ø1D DRP ENDNODE Hello S=7.288 BLKS
58 Ø.ØØ16 Jeff Alice NCP C F=B4B5 Read 512 at 39936
59 Ø.ØØ7Ø Alice Jeff NCP R OK 512 bytes read
6Ø Ø.Ø1Ø6 Jeff Alice NCP C F=B4B5 Read 512 at 4Ø448
61 Ø.ØØ7Ø Alice Jeff NCP R OK 512 bytes read
62 Ø.Ø1Ø4 Jeff Alice NCP C F=B4B5 Read 512 at 87Ø4Ø
63 Ø.ØØØ4 Broadcast DG ØF Ø1Ø9 Netmap IP=[128.158.2.5Ø] Version
64 Ø.ØØ99 Alice Jeff NCP R OK 512 bytes read
65 Ø.Ø199 Jeff Alice NCP C F=B4B5 Write 512 at Ø
66 Ø.ØØ48 Alice Jeff NCP R OK
67 Ø.ØØ2Ø Jeff Alice NCP C F=B4B5 Read 512 at Ø
68 Ø.ØØ72 Alice Jeff NCP R OK 512 bytes read
69 Ø.Ø139 Jeff Alice NCP C F=B4B5 Write 512 at 7Ø656
7Ø Ø.ØØ56 Alice Jeff NCP R OK
71 Ø.ØØ21 Jeff Alice NCP C F=B4B5 Read 512 at 7Ø656
72 Ø.ØØØ7 LTM listnrs DEC Ø94374 Ethertype=8Ø3F (DEC LAN moni
73 Ø.ØØ61 Alice Jeff NCP R OK 512 bytes read
74 Ø.Ø142 Jeff Alice NCP C F=B4B5 Write 512 at 87Ø4Ø
75 Ø.ØØ5Ø Alice Jeff NCP R OK
Frame 75 of 5847
1 Help
2 Set mark
5 Menus
6Disply options
7 Prev frame
8 Next frame
9Select frame
1Ø New capture

Figure 7–22. Sample Summary view

How information is displayed, and *how much* information is shown in the Summary view depends on which display options are enabled, as described in "The Summary View Display Options" on page 7–35.

Tthe Summary view always shows frame numbers and either station names (if the names correspond to addresses in the name table) or numeric addresses (if they do not). (For information about maintaining the name table, see "Managing Names" on page 8–3.)

Numeric Addresses in the Summary View

If a numeric address is shown, it appears in the conventional format for its type. For example, a DLC address is shown in hexadecimal, an IP address is shown as ***[n.n.n.n]***, and so on. On Ethernet or token ring, each station's DLC address contains six bytes,

which are written as 12 hexadecimal digits. The default is to display the highest-level protocol address.

To display other protocol addresses, you must enable the desired protocol levels in the **Address level** filter, as described in "Address Level Filter" on page 7–8. To display DLC addresses, enable the **DLC addresses** option.

On ARCNET, the first two bytes contain the source and destination. The next two bytes are shown as an integer representing the frame's total length. This is actually a simplification of what is actually transmitted on the network. ARCNET uses two different formats; one for short frames and another for long frames. A short frame has a 1-byte length. A particular value in the first byte means that a second byte is present. (As a side effect of this implementation, certain frame lengths are illegal.) The Sniffer Network Analyzer evaluates the length according to the ARCNET convention. However, it records all frames in the same format, using a 2-byte length field.

The analyzer replaces the one or two bytes that were actually transmitted with a standard 2-byte representation. In this respect, what the analyzer records is not an exact replica of the transmission. However, it greatly simplifies the task of pattern matching, since the data field starts at the same offset in all recorded ARCNET frames.

Display of Manufacturers' IDs

You can choose whether or not to display the first three bytes of a station's DLC address as the manufacturer's ID. If this option is enabled, then the analyzer attempts to interpret the first three bytes of the address as the name of the manufacturer of the adapter card. If the manufacturer's code is in the manufacturer's table, that code replaces the first six characters of the station address with an ASCII abbreviation of the manufacturer's name. If this option is not enabled, the display shows the first three bytes of the DLC address without translating them.

NOTE: The file that contains the names for Manufacturers' IDs is named STARTUP.*xx*I (where *xx* is a two-letter network abbreviation, such as TR or EN). For an overview of this table, see Figure 11–8 on page 11–17.

Name Width Display Option

You can define the width of the name field in the summary view, from 6 characters up to 31 characters (the default is 15 characters). For example, if you use long names, you may want to make the name field wider to accommodate the names. This option also affects the Expert view.

On ARCNET or LocalTalk, a DLC address consists of a single byte. On Ethernet, StarLAN, PC Network, or token ring, each station's address contains six bytes, which can be written as 12 hexadecimal characters.

If the display includes a name longer than the specified name width, the Sniffer analyzer truncates that name and replaces its last two visible characters with dots (to show that the name has been truncated). For example, if the **Name width** option specifies an 8-character field and you enter the 10-character name **"FileServer,"** the Summary view would show **"FileSe . . "**

The Summary View Display Options

Figure 7–23 provides an overview of the default Summary view display options. As you can see, all options are disabled except the **Delta time** option. (This configuration gives you a display like the one in Figure 7–22.) If you enable all the options, you must scroll horizontally to see all of the resulting display. If you use a larger, external screen, you may be able to display more rows or columns.

NOTE: For ARCNET, you can also choose between displaying addresses as Hex or Octal values.

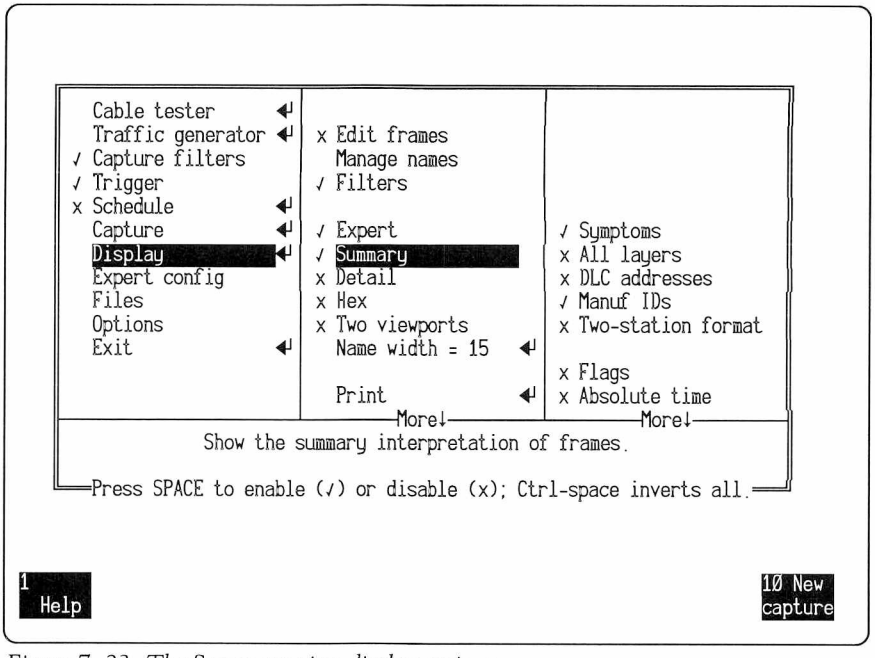


Figure 7–23. The Summary view display options

The first five display options determine *how* information is displayed. The sections that follow describe each option in more detail.

Symptoms — If enabled, the summary view shows the last symptom found (if any) for each frame.

All layers — If enabled, the Summary view shows one line for each protocol level contained in a frame. If disabled, only one line—for the highest enabled protocol level—is shown. The default is **All layers** disabled (x).

DLC addresses — If enabled, the Summary view shows the DLC address for each displayed frame, even if several protocol levels are shown (**All layers** enabled). If disabled, the address associated with the highest level protocol is shown. The default is **DLC addresses** disabled (x).

Manuf IDs — If enabled, the Summary view shows the first three bytes of a station's DLC address as the manufacturer's name. If disabled, the Summary view shows the bytes without translating them into the manufacturer's ID.

Two-station format — If enabled, displays only traffic between two stations.

The rest of the display options determine *whether* each of the following is displayed. The default is all options disabled, except for **Delta time**.

Flags — Shows flags associated with a frame.

Absolute time — Shows when the frame was received.

Delta time — Shows the interval between the current frame and the previous frame.

Relative time — Shows the interval between the current frame and the marked frame.

Bytes — Shows the frame's length.

Cumulative bytes — Shows the length of all frames, starting with the marked frame and including the current frame.

NW utilization — Shows an estimate of the percentage of the network's bandwidth devoted to transmitting the displayed frame.

All Layers Display Option

This option determines whether the Summary view shows a single line that identifies only the frame's highest protocol level or whether it shows a separate line for each interpreted protocol level[1]. If you disable the **All layers** option, the lowest level appears on top of the others. How addresses appear also depends on the **DLC**

addresses option. If that option is disabled, the address associated with the highest level is automatically shown. On a color monitor, each level is color coded (see "About the Use of Color" on page 7–29).

Figure 7–24 shows a Summary view with **All layers** and **DLC addresses** enabled. Figure 7–25 shows a view with **All layers** and **DLC addresses** disabled.

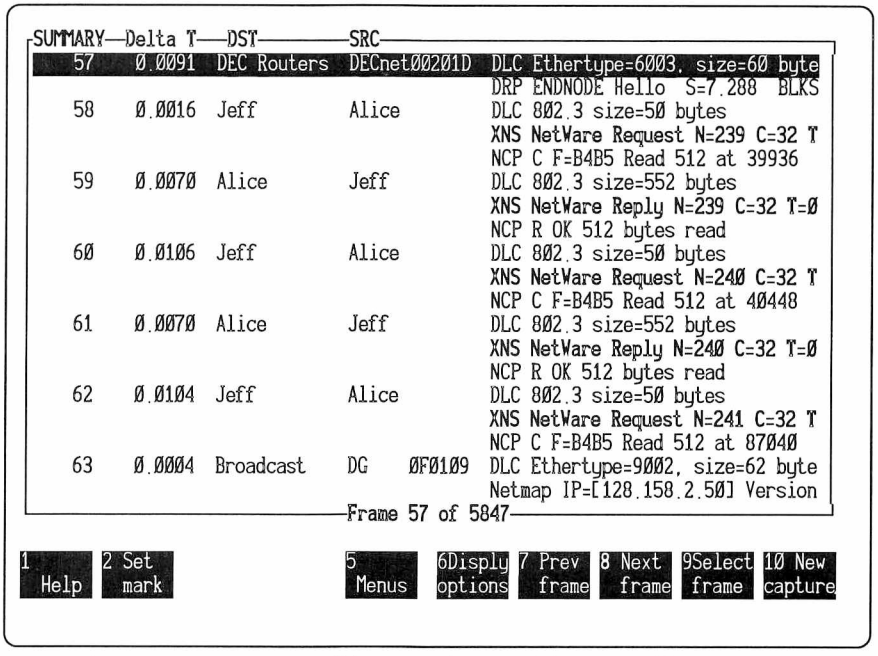

SUMMARY—Delta T——DST————SRC
57 Ø.ØØ91 DEC Routers DECnetØØ2Ø1D DLC Ethertype=6ØØ3, size=6Ø byte
DRP ENDNODE Hello S=7.288 BLKS
58 Ø.ØØ16 Jeff Alice DLC 8Ø2.3 size=5Ø bytes
XNS NetWare Request N=239 C=32 T
NCP C F=B4B5 Read 512 at 39936
59 Ø.ØØ7Ø Alice Jeff DLC 8Ø2.3 size=552 bytes
XNS NetWare Reply N=239 C=32 T=Ø
NCP R OK 512 bytes read
6Ø Ø.Ø1Ø6 Jeff Alice DLC 8Ø2.3 size=5Ø bytes
XNS NetWare Request N=24Ø C=32 T
NCP C F=B4B5 Read 512 at 4Ø448
61 Ø.ØØ7Ø Alice Jeff DLC 8Ø2.3 size=552 bytes
XNS NetWare Reply N=24Ø C=32 T=Ø
NCP R OK 512 bytes read
62 Ø.Ø1Ø4 Jeff Alice DLC 8Ø2.3 size=5Ø bytes
XNS NetWare Request N=241 C=32 T
NCP C F=B4B5 Read 512 at 87Ø4Ø
63 Ø.ØØØ4 Broadcast DG ØF91Ø9 DLC Ethertype=9ØØ2, size=62 byte
Netmap IP=[128.158.2.5Ø] Version
Frame 57 of 5847
1 Help
2 Set mark
5 Menus
6Disply options
7 Prev frame
8 Next frame
9Select frame
1Ø New capture

Figure 7–24. Summary view, All layers and DLC addresses enabled

1. In X Windows, there is a separate line for each protocol of each message within the frame.

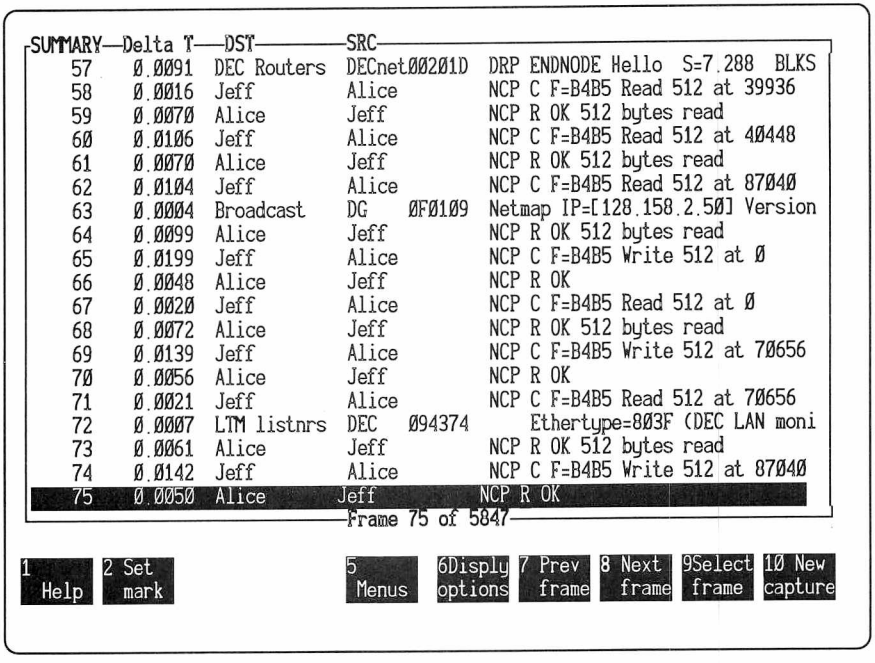

SUMMARY—Delta T—DST—SRC
57 0.0091 DEC Routers DECnet00201D DRP ENDNODE Hello S=7.288 BLKS
58 0.0016 Jeff Alice NCP C F=B4B5 Read 512 at 39936
59 0.0070 Alice Jeff NCP R OK 512 bytes read
60 0.0106 Jeff Alice NCP C F=B4B5 Read 512 at 40448
61 0.0070 Alice Jeff NCP R OK 512 bytes read
62 0.0104 Jeff Alice NCP C F=B4B5 Read 512 at 87040
63 0.0004 Broadcast DG 0F0109 Netmap IP=[128.158.2.50] Version
64 0.0099 Alice Jeff NCP R OK 512 bytes read
65 0.0199 Jeff Alice NCP C F=B4B5 Write 512 at 0
66 0.0048 Alice Jeff NCP R OK
67 0.0020 Jeff Alice NCP C F=B4B5 Read 512 at 0
68 0.0072 Alice Jeff NCP R OK 512 bytes read
69 0.0139 Jeff Alice NCP C F=B4B5 Write 512 at 70656
70 0.0056 Alice Jeff NCP R OK
71 0.0021 Jeff Alice NCP C F=B4B5 Read 512 at 70656
72 0.0007 LTM listnrs DEC 094374 Ethertype=803F (DEC LAN moni
73 0.0061 Alice Jeff NCP R OK 512 bytes read
74 0.0142 Jeff Alice NCP C F=B4B5 Write 512 at 87040
75 0.0050 Alice Jeff NCP R OK
Frame 75 of 5847
1 Help
2 Set mark
5 Menus
6Disply options
7 Prev frame
8 Next frame
9Select frame
10 New capture

Figure 7–25. Summary view, All layers and DLC addresses disabled

To define the displayed protocol levels in Summary view:

1. Move to **Display\Summary\All layers**. Press Spacebar to enable (√) or disable (x) the option.

DLC Addresses Display Option

This option determines whether the DLC address or the address associated with the highest-level protocol is shown in the Summary view. If the option is disabled, the highest-level address is shown. If it is enabled, the DLC address is shown even if you display all protocol layers. Figure 7–25, for example, shows the highest layer—the result of disabling the **DLC addresses** option.

Manufacturers' IDs Display Option

You can choose whether or not the Summary view will display the first three bytes of a station's DLC address as the manufacturer's ID or as hex characters. This feature is enabled by default; to toggle the setting, move to **Display/Summary/Manuf IDs** and press the Spacebar.

Two-Station Format Display Option

When you examine network activity, you often want to focus on traffic between a pair of stations. To do this, you can set up filters that define the two stations (see "Station Address Display Filter" on page 7–11) and enable the **Two-station format** option.

NOTE: If you do not set these filters, the Sniffer analyzer accepts other frames as well and displays those frames in the usual format. Since this is inconsistent with the two-station format, it makes the feature less useful.

The two-station format shows transmissions from one station (the station that was detected first) on the left side of the screen and transmissions from the other station on the right, as shown in Figure 7–26. The source and destination fields are omitted. Instead, there are two columns, headed **From *xxx*** and **From *yyy***. A frame from the station on the left is assumed to be addressed to the station on the right, and vice versa.

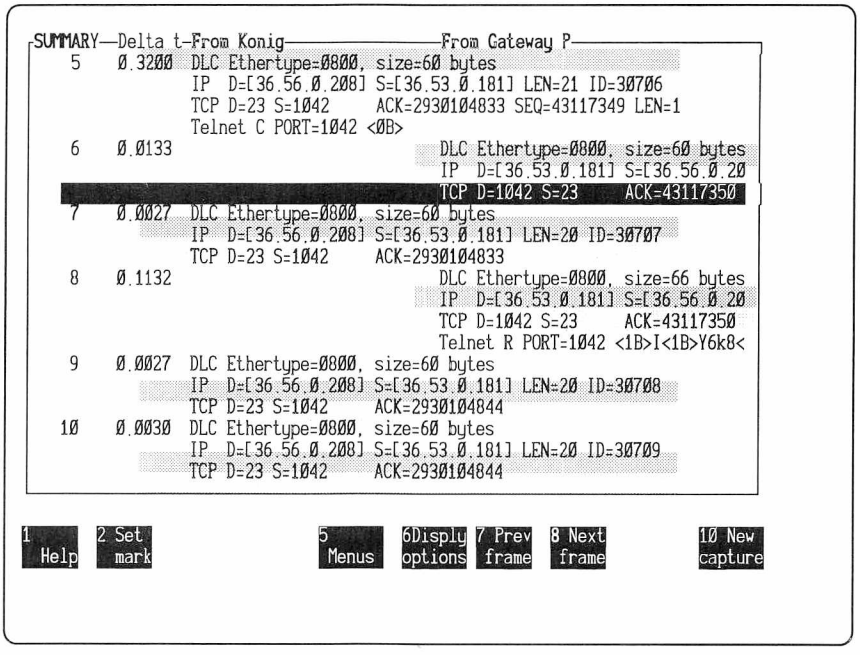

SUMMARY—Delta t—From Konig—From Gateway P
5 0.3200 DLC Ethertype=0800, size=60 bytes
IP D=[36.56.0.200] S=[36.53.0.181] LEN=21 ID=30706
TCP D=23 S=1042 ACK=2930104833 SEQ=43117349 LEN=1
Telnet C PORT=1042 <0B>
6 0.0133 DLC Ethertype=0800, size=60 bytes
IP D=[36.53.0.181] S=[36.56.0.20
TCP D=1042 S=23 ACK=43117350
7 0.0027 DLC Ethertype=0800, size=60 bytes
IP D=[36.56.0.200] S=[36.53.0.181] LEN=20 ID=30707
TCP D=23 S=1042 ACK=2930104833
8 0.1132 DLC Ethertype=0800, size=66 bytes
IP D=[36.53.0.181] S=[36.56.0.20
TCP D=1042 S=23 ACK=43117350
Telnet R PORT=1042 <1B>I<1B>Y6k8<
9 0.0027 DLC Ethertype=0800, size=60 bytes
IP D=[36.56.0.200] S=[36.53.0.181] LEN=20 ID=30708
TCP D=23 S=1042 ACK=2930104844
10 0.0030 DLC Ethertype=0800, size=60 bytes
IP D=[36.56.0.200] S=[36.53.0.181] LEN=20 ID=30709
TCP D=23 S=1042 ACK=2930104844
1 Help
2 Set mark
5 Menus
6Disply options
7 Prev frame
8 Next frame
10 New capture

Figure 7–26. Two-station format for the Summary view

To use the two-station format:

1. Set the **Station address** filters to display only the two stations of interest.
2. Move to **Display \ Summary \ Two-Station Format** and press Spacebar to enable (√) the option.

3. To adjust the separation between the columns, change the **Name width** option.
4. To adjust the display's horizontal position, use the horizontal Cursor keys to scroll sideways.

Flags Display Option

If you enable the **Flags** option, the analyzer displays up to six of the flags associated with a frame. (Figure 7–27 shows the **Selected frame** flag for frame 64.)

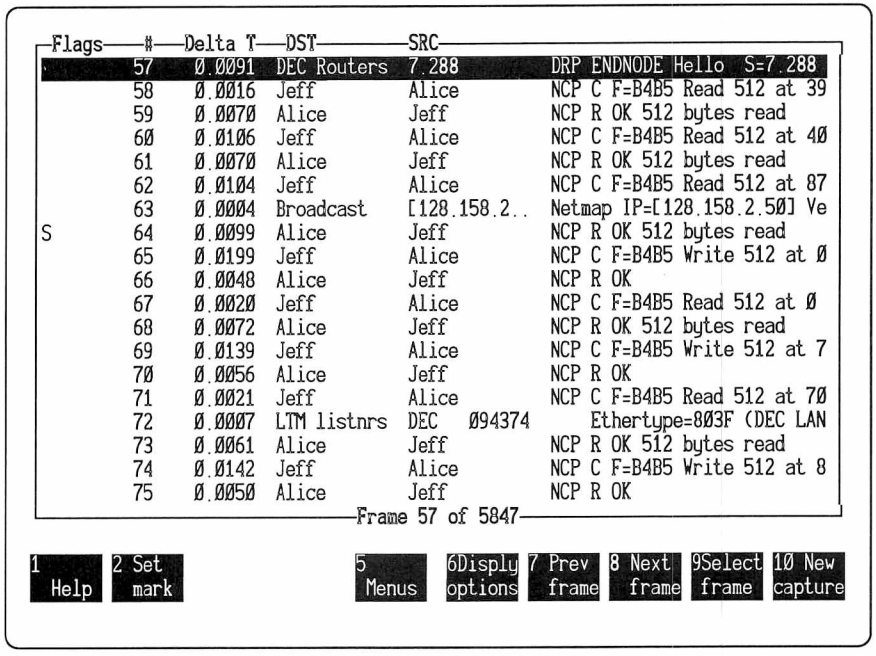

Flags # Delta T DST SRC
57 0.0091 DEC Routers 7.288 DRP ENDNODE Hello S=7.288
58 0.0016 Jeff Alice NCP C F=B4B5 Read 512 at 39
59 0.0070 Alice Jeff NCP R OK 512 bytes read
60 0.0106 Jeff Alice NCP C F=B4B5 Read 512 at 40
61 0.0070 Alice Jeff NCP R OK 512 bytes read
62 0.0104 Jeff Alice NCP C F=B4B5 Read 512 at 87
63 0.0004 Broadcast [128.158.2.. Netmap IP=[128.158.2.50] Ve
S 64 0.0099 Alice Jeff NCP R OK 512 bytes read
65 0.0199 Jeff Alice NCP C F=B4B5 Write 512 at 0
66 0.0048 Alice Jeff NCP R OK
67 0.0020 Jeff Alice NCP C F=B4B5 Read 512 at 0
68 0.0072 Alice Jeff NCP R OK 512 bytes read
69 0.0139 Jeff Alice NCP C F=B4B5 Write 512 at 7
70 0.0056 Alice Jeff NCP R OK
71 0.0021 Jeff Alice NCP C F=B4B5 Read 512 at 70
72 0.0007 LTM listnrs DEC 094374 Ethertype=803F (DEC LAN
73 0.0061 Alice Jeff NCP R OK 512 bytes read
74 0.0142 Jeff Alice NCP C F=B4B5 Write 512 at 8
75 0.0050 Alice Jeff NCP R OK
Frame 57 of 5847
1 Help
2 Set mark
5 Menus
6Disply options
7 Prev frame
8 Next frame
9Select frame
10 New capture

Figure 7–27. Displaying flags in the Summary view

NOTE: Three of the flags listed below (M, E, and S) are displayed whether or not **Flags** is enabled. The remaining flags are displayed only if you enable the **Flags** option.

Flags include:

M — Mark—the reference frame for relative time or cumulative bytes. To set the mark on the current frame, press F2 **[Set mark]**.

T — Trigger—the frame defined as the trigger event, which contains the specified pattern that stops the capture.

↓	Protocol forced—the rules associated with the protocol forcing feature apply to this frame (see "Specifying a Protocol Forcing Rule" on page 9–4). If there are multiple arrows, each indicates one force (up to six recursions).
E	Edited—this frame was edited.
S	Selected frame—you selected this frame. To select a frame, move to it and press F9 **[Select frames]**. By also enabling the **Selected frames** display filter, you can collect selected frames and save them to a file, as described in greater detail in "Selected Frames Display Filter" on page 7–16.
C	CRC (Ethernet)—a frame whose CRC does not agree with the actual bytes received, which suggests that it contains invalid characters.
R	Short/Runt (Ethernet)—a frame that is less than 60 bytes, which may indicate a collision.
L	Lost frame (Ethernet)— the frames that preceded this frame reached the network interface card but were lost before they reached the capture buffer.
O	Overrun (Ethernet)—the frame that preceded this frame was discarded because of an error during transfer from the network to the capture buffer. This may happen during high-volume traffic with small frames.
X	Collision (Ethernet-II only)—the frame that preceded this frame is the result of a collision. This flag is applied only if the collision occurred after the frame's preamble.
A	Abort—(WAN/Synchronous) the frames that immediately preceded this frame were aborted by the sender.

"Time" and "Volume" Display Options

To examine a network's throughput, you need to know about the volume and timing of transmissions. For every frame, you can include or omit various indicators of the time or the flow of data, including:

- Absolute time
- Delta time
- Relative time

- Bytes
- Cumulative bytes
- Network utilization

Figure 7–28 shows a Summary view with all options (except network utilization) enabled.

If you enable all the options, the display may be wider than the screen. If that happens, use the Cursor keys to scroll sideways to see the entire display.

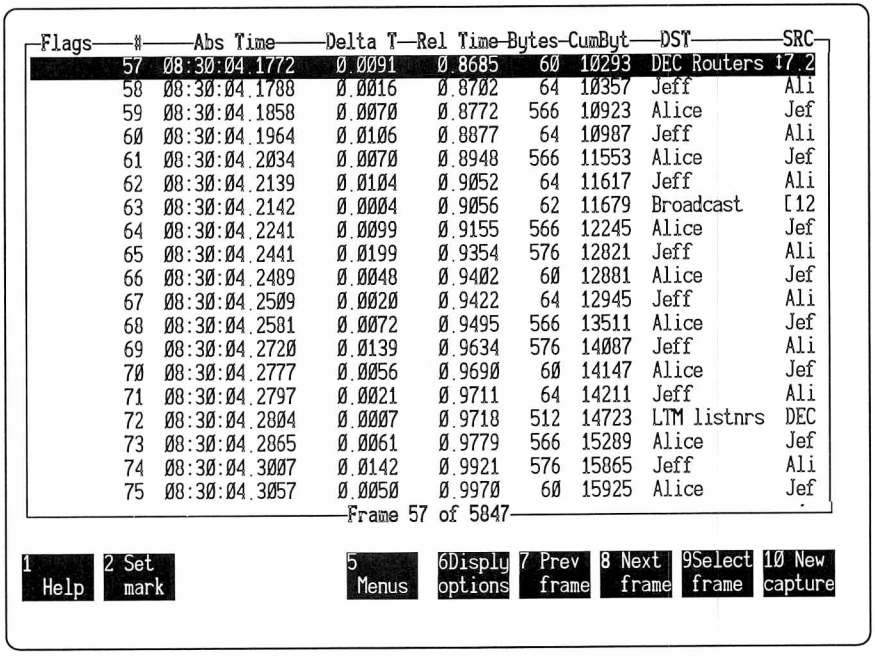


Figure 7–28. Displaying time and traffic volume information

Absolute time

Absolute time shows when the last byte of a frame was received. At that time, the Sniffer analyzer attaches the timestamp based on its internal clock. All other time displays are based on this value. On networks other than token ring, **Absolute time** is displayed to the nearest tenth of a millisecond. On token ring, it is displayed to the nearest millisecond.

Absolute time also appears in the Detail view.

Delta time

Delta time shows the interval between the current frame's timestamp and that of the preceding frame. Because Delta time shows the interval to the preceding displayed frame, frames that are not displayed do not affect Delta time.

NOTE: You can use the **Frame editing** feature to change this value.

Relative time

Relative time shows the difference between the current frame's timestamp and the timestamp of the reference frame, which is marked with the "M" flag (see "Flags Display Option" on page 7–40). When you first display the buffer, the first frame is the marked frame.

You can set this flag by pressing F2 **[Set mark]** while the desired frame is highlighted. This removes the flag from the currently marked frame. Once you mark a reference frame, you can find it quickly (see "Jumping to the Marked Frame" on page 7–60).

Bytes

Bytes shows the total number of bytes in the frame, not including the CRC frame.

Cumulative bytes

Cumulative bytes shows the sum of the lengths of the displayed frames, from the reference frame (flagged "M") through the current frame (including both). If you did not redefine the reference frame, the analyzer counts from the first displayed frame.

You can choose to display either the **Cumulative bytes** or the **Network utilization** option. The analyzer will not let you enable both options.

Network utilization

Network utilization shows an estimate of the percentage of the network's bandwidth devoted to transmitting the displayed frame (and perhaps those preceding and following it). The measurement is:

$$\frac{100 \times \textit{bytes in all frames accepted during the interval}}{\textit{Theoretical maximum frames transmitted during the interval}}$$

The interval is a time window centered around the frame. You can set the size of the interval to 1, 10, 100, or 1000 milliseconds. For example, if you pick 100 millisecond intervals, the utilization for a frame that arrived at 13:27:06.100 is based on the number of bytes in frames whose arrival times ranged from 13:27:06.050 to 13:27:06.150.

Utilization is a moving average. With a smaller interval, you'll see larger momentary fluctuations. A larger interval, however, smooths them out. Any measure of network utilization must be based on a time window, whether described explicitly or not. Viewed without window averaging, a network is always either 100 percent busy (when a frame is being transmitted) or 0 percent busy (when no frame is being transmitted).

The Detail View

The Detail view (Figure 7–29) presents a complete interpretation of a frame for each field and the associated parameters. It also shows some information not contained within the frame, such as the absolute time, which shows when the frame arrived.

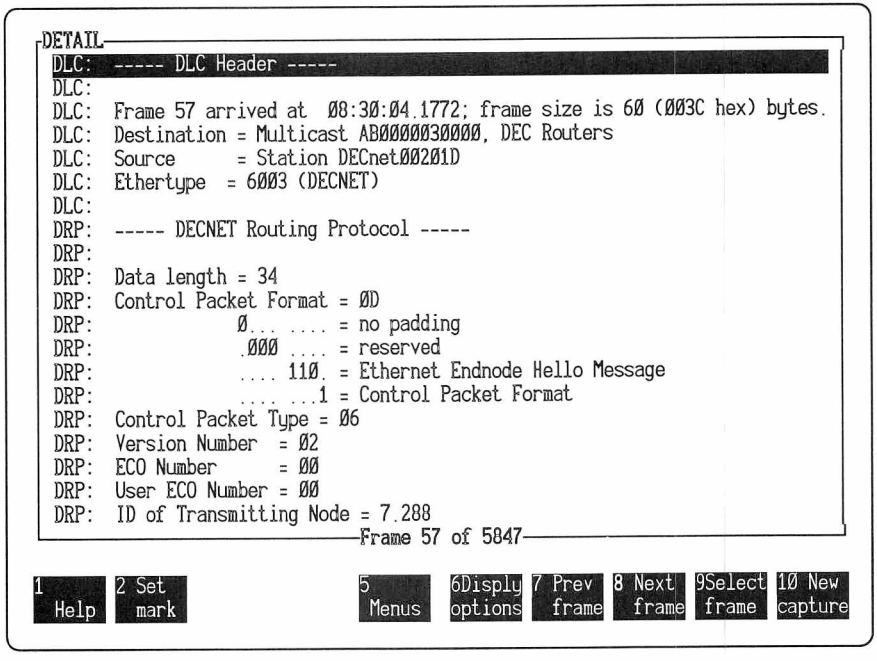

DETAIL
DLC: ----- DLC Header -----
DLC:
DLC: Frame 57 arrived at 08:30:04.1772; frame size is 60 (003C hex) bytes.
DLC: Destination = Multicast AB000000300000, DEC Routers
DLC: Source = Station DECnet00201D
DLC: Ethertype = 6003 (DECNET)
DLC:
DRP: ----- DECNET Routing Protocol -----
DRP:
DRP: Data length = 34
DRP: Control Packet Format = 0D
DRP: 0... .... = no padding
DRP: .000 .... = reserved
DRP: .... 110. = Ethernet Endnode Hello Message
DRP: ....1 = Control Packet Format
DRP: Control Packet Type = 06
DRP: Version Number = 02
DRP: ECO Number = 00
DRP: User ECO Number = 00
DRP: ID of Transmitting Node = 7.288
Frame 57 of 5847
1 Help
2 Set mark
5 Menus
6Disply options
7 Prev frame
8 Next frame
9Select frame
10 New capture

Figure 7–29. Sample Detail view

Because the Detail view includes so many lines, you can only see a partial view at any one time. The left margin shows which protocol governs that portion of the interpretation. To see another section of the view, you can scroll with the Cursor keys or use the **Search** function (see "Searching for Text" on page 7–57).

When you print the Detail view, the analyzer prints the entire text of the open view (or views), regardless of screen boundaries.[1] Figure 7–30 shows the Detail view as it

1. Depending on how you configured your system, you can redirect printer output elsewhere.

appears when printed. (For information about printing, see "Printing and Importing Data" on page 7–60.)

```
DLC:  ----- DLC Header -----
DLC:
DLC:  Frame 74 arrived at  14:29:40.1033; frame size is 73 (0049 hex) bytes.
DLC:  FS: Addr recognized indicator: 0, Frame copied indicator: 0
DLC:  FC: SMT Info Frame
DLC:  Destination = Station Syner 0020C0
DLC:  Source      = Station Syner 002080
DLC:
SMT: ----- FDDI Station Management -----
SMT:
SMT: Frame class = 1 (Neighbor info)   Frame type = 3 (Response)
SMT: Version ID = 1, transaction ID = B
SMT: This station address = 0 Syner 002000 , length = 40
SMT: Upstream neighbor address =  Syner 0020C0
SMT: Station descriptor:
SMT:     Node class       = Concentrator
SMT:     MAC count        = 3
SMT:     Non-master count = 2
SMT:     Master count     = 8
SMT: Station state descriptor
SMT:     Topology = 31
SMT:          .... ...1 = Station wrapped
SMT:          ...1 .... = Rooted station
SMT:          ..1. .... = Status reporting
SMT:     Duplicate Address = 00
SMT:          .... .... = (none)
SMT: Frame status capabilities for MAC 1 = 0000
SMT:          .... .... .... .... = (none)
```

Figure 7–30. Sample of complete Detail view information when printed

Protocol Layers in the Detail View

When a frame contains several protocol layers, the Detail view interprets all the layers. The outermost (lowest) layer appears first, followed by any other layers until the innermost (highest) layer, which appears last.

Scrolling in the Detail View

Because the interpretation in the Detail view is often larger than the screen, you can scroll to see the entire display.

When both the Summary and Detail views are displayed, scrolling depends on the display options you choose.

Controlling the Layer Displayed in the Detail View

If you enable the **All layers** option for the Summary view, the analyzer automatically scrolls to show the highest level in the Detail view. If a frame does not include the

layer you selected, the next lower layer is highlighted. If the option is disabled, the analyzer scrolls to match the level highlighted in the Summary view.

To set the level initially displayed in the Detail view:

1. Move to **Display\Summary\All layers** and press Spacebar to enable (√) the option.
2. In the Summary view, move to the level you want to display in the Detail view.

Maintaining Cursor Position in the Detail View

If you want to see the decode for a particular protocol in more than one frame, enable the **Maintain Position** option for the Detail view. When you enable (√) it, the Detail view will display the same protocol as you move from frame to frame. (If the protocol you want to see is not present in a frame, the Detail view will show the first line of the highest protocol.) When you exit the Display window, the analyzer resets its position.

- When **Maintain Position** is disabled, the Detail view displays the highest protocol as you move between frames.
- When **Maintain Position** is enabled, the Detail view displays the same protocol as you move from frame to frame. The analyzer "remembers" which area of the Detail view is highlighted, and it highlights the same area (protocol and offset) for the next frame.

To maintain cursor position in the Detail view:

1. Move to **Display\Detail\Maintain Position** and press Spacebar to enable (√) the option.
2. In the Detail view, move to the decode you want to display. Press F7 **[Previous Frame]** or F8 **[Next Frame]** to see that decode for other frames. If you move to the Summary view, move to another frame and then return to the Detail view, the cursor will return to a position in the same general area of the frame.

Formats for Higher-Level Numeric Addresses

In the Detail view, the analyzer shows the numeric form of each source or destination address, as well as the name assigned to that address in the name table.

The numeric display format of higher-level addresses is hexadecimal, except when there is an established convention for a different form. For example, a 4-byte IP address is shown as a succession of four decimal numbers separated by dots, with the entire number enclosed in square brackets.

For each displayed address, a format appropriate to the level and protocol for that address is shown. Figure 7–32 shows examples of common address formats.

	Ethernet, Token Ring, StarLAN, PC Network, FDDI	ARCNET, LocalTalk	Sniffer Internetwork Analyzer (WAN/Synchronous)
DLC	Shows all frames as 12 hexadecimal digits, corresponding to the 6-byte address. Ex: 020701031EF7	Shows all frames as two hexadecimal digits, corresponding to the 1-byte address. Ex: 3C	Shows each frame as either from DTE or from DCE.
XNS	Format is the same as a 6-byte DLC address. (Although an XNS address may be the same as a DLC address, the analyzer does not attempt to interpret the manufacturer's ID, as in the DLC address.) Ex. 0000404.00001B30F09A		
IP	Address is represented byte by byte. Each byte is shown as a decimal value; a number between 0 and 255. Successive bytes are separated by a dot, and the whole sequence is enclosed in brackets. Ex. [84.12.139.144]		
DRP (DECnet)	Address is represented by two decimal numbers, the *area* and the *node number*, separated by a dot. Each number is computed as the binary value after masking certain bits in the address. Ex. 184.27		
DDP (AppleTalk)	Address is represented by two decimal numbers, the network number (representing a 16-bit network address) and the node ID (representing an 8-bit node number), separated by a dot. Ex. 1080.208		
IPX	Address is represented by two address types, a 4-byte network number and a 6-byte node address, separated by a dot. Ex. 00000007.723259223502		

Figure 7–31. Address formats for selected networks and protocols

The Hexadecimal View

The Hex view displays each byte as two hex characters, 00 to FF, with a blank between successive bytes. The bytes are arranged 16 to a row in a full-width table (eight to a row in the half-width table for the **Two viewports** option).

As shown in Figure 7–32, the far left column shows the offset from the beginning of the frame, which allows you to readily calculate each field's address. The hexadecimal offset is required when you describe a pattern to be matched. You can "copy and paste" the offset pattern from a displayed frame, without having to type the offset. For more

information, see "Copying and Pasting a Pattern from the Display Hex Window" on page 6–55.

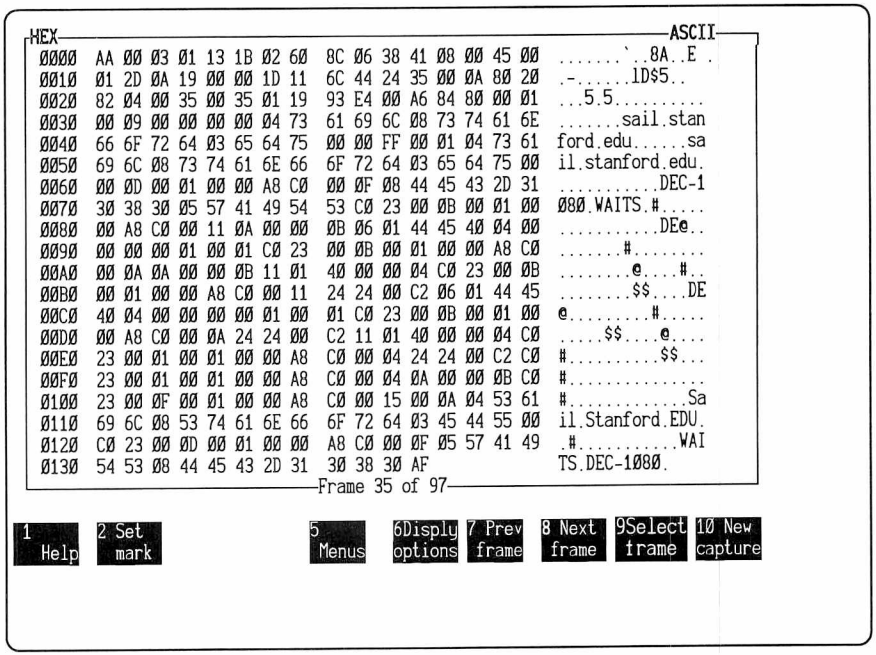


Figure 7–32. Hexadecimal view of a TCP/IP frame on Ethernet

If both the Detail and Hex views are displayed, moving the highlight in the Detail view automatically highlights the corresponding bytes in the Hex view, as shown in Figure 7–33. This makes it easy to match a sequence of bytes with the interpretation of those bytes.

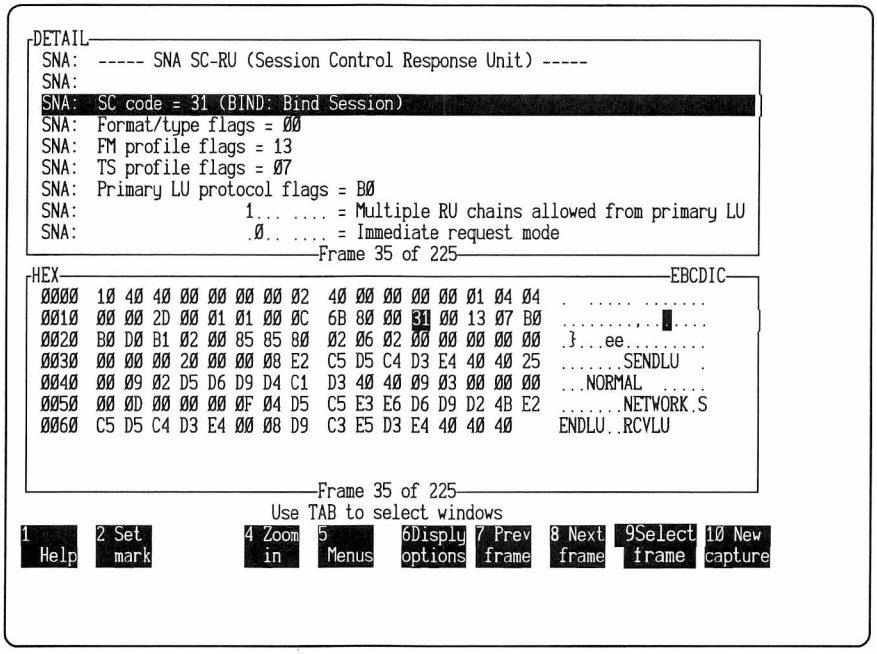

DETAIL
SNA: ----- SNA SC-RU (Session Control Response Unit) -----
SNA:
SNA: SC code = 31 (BIND: Bind Session)
SNA: Format/type flags = 00
SNA: FM profile flags = 13
SNA: TS profile flags = 07
SNA: Primary LU protocol flags = B0
SNA: 1... .... = Multiple RU chains allowed from primary LU
SNA: .0.. .... = Immediate request mode
Frame 35 of 225
HEX
EBCDIC
0000 10 40 40 00 00 00 00 02 40 00 00 00 00 01 04 04 . ...
0010 00 00 2D 00 01 01 00 0C 6B 80 00 31 00 13 07 B0 .....,..k..1....
0020 B0 D0 B1 02 00 85 85 80 02 06 02 00 00 00 00 00 .}...ee.....
0030 00 00 00 20 00 00 08 E2 C5 D5 C4 D3 E4 40 40 25 .....SENDLU .
0040 00 09 02 D5 D6 D9 D4 C1 D3 40 40 09 03 00 00 00 ...NORMAL .....
0050 00 0D 00 00 00 0F 04 D5 C5 E3 E6 D6 D9 D2 4B E2 .....NETWORK.S
0060 C5 D5 C4 D3 E4 00 08 D9 C3 E5 D3 E4 40 40 40 ENDLU..RCVLU
Frame 35 of 225
Use TAB to select windows
1 Help
2 Set mark
4 Zoom in
5 Menus
6Disply options
7 Prev frame
8 Next frame
9Select frame
10 New capture

Figure 7–33. Synchronized highlighting in the Detail and Hex views

Display of Spanned Frames

In some protocols, a message at one of the higher levels may span several DLC frames. During display, the Detail view reassembles the entire high-level message as though the whole message were in the first frame. This allows you to read the message without having to jump among the frames that contain its parts. When you highlight a part of the Detail view, the Hex view continues to highlight the corresponding hex characters.

Figure 7–34 illustrates the treatment of a spanned high-level message.

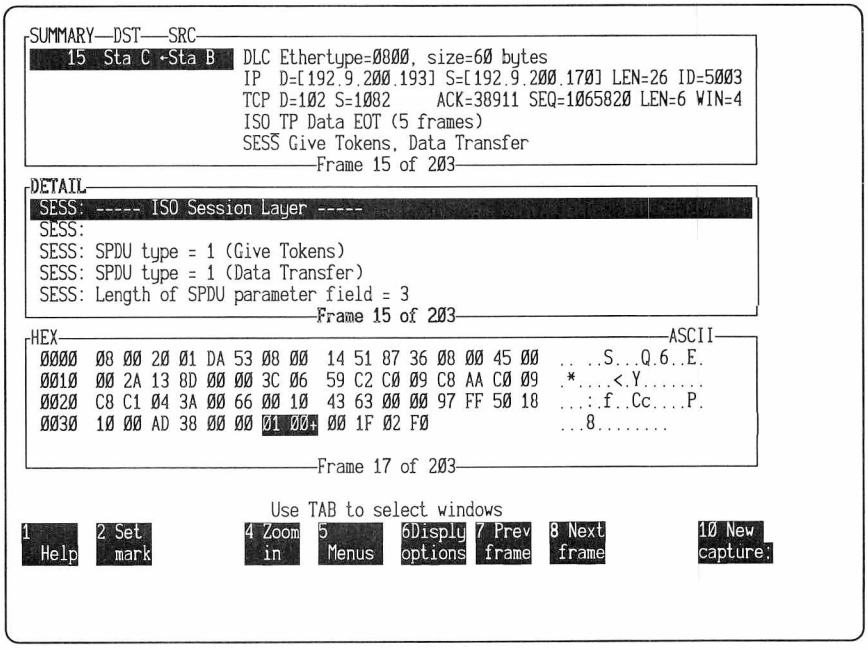

SUMMARY—DST—SRC
15 Sta C ←Sta B DLC Ethertype=0800, size=60 bytes
IP D=[192.9.200.193] S=[192.9.200.170] LEN=26 ID=5003
TCP D=102 S=1082 ACK=38911 SEQ=1065820 LEN=6 WIN=4
ISO TP Data EOT (5 frames)
SESS Give Tokens, Data Transfer
Frame 15 of 203
DETAIL
SESS: ----- ISO Session Layer -----
SESS:
SESS: SPDU type = 1 (Give Tokens)
SESS: SPDU type = 1 (Data Transfer)
SESS: Length of SPDU parameter field = 3
Frame 15 of 203
HEX ASCII
0000 08 00 20 01 DA 53 08 00 14 51 87 36 08 00 45 00 .. ..S...Q.6..E.
0010 00 2A 13 8D 00 00 3C 06 59 C2 C0 09 C8 AA C0 09 .*....<.Y.....
0020 C8 C1 04 3A 00 66 00 10 43 63 00 00 97 FF 50 18 ...:.f..Cc....P.
0030 10 00 AD 38 00 00 01 00+ 00 1F 02 F0 ...8.....
Frame 17 of 203
Use TAB to select windows
1 Help
2 Set mark
4 Zoom in
5 Menus
6Disply options
7 Prev frame
8 Next frame
10 New capture

Figure 7–34. Detail and Hex view of a spanned ISO frame

Here are some points to observe:

- In the Summary view, the frame in which the high-level message starts includes a note that informs you how many frames are spanned by that message. In Figure 7–34, for example, the note "ISO_TP Data EOT (5 frames)" indicates where the ISO TP data was split among frames 15, 16, 17, 18, 19, and 20. There is no presumption that spanned frames are consecutive; unrelated frames might have arrived between them and so appear interspersed in the display.
- In the Detail view, the entire high-level message is displayed as though all of it were in the frame in which it starts. When you print the display, the entire high-level message appears without a break, in as many lines as necessary. On the screen, you can see the rest of the message by scrolling within the Detail view.
- The frame number in the Hex view does not necessarily match the frame number in the Detail view. In Figure 7–34, the interpretation of ISO Session Layer is part of the Detail view of frame 15 because that is where the ISO TP data starts. However, the corresponding Hex view shows frame 17 because—although the message started in frame 15—its ISO Session Layer continues to frame 17, starting at offset 36.
- When the field highlighted in the Detail view extends over additional frames, the Hex panel scrolls to the start of the corresponding field, but adds a + sign to show that there is additional information in a different frame.

The Hexadecimal View Display Options

As with the Summary view display options, the Hex view display options determine how data is displayed. These options include:

- Type of interpretation
- Whether to ignore the high bit as a parity bit

Defining the Type of Interpretation

To the right of the hexadecimal codes, the Hex view shows the corresponding ASCII or EBCDIC characters. A standard character is shown by its text equivalent; anything else is represented by a dot.

The interpretation of characters follows either ASCII or EBCDIC conventions. For Ethernet and token ring networks, you can also choose **Dynamic mode**, which automatically adjusts interpretation for each frame as either EBCDIC (for all MAC frames and for any LLC frames whose SAP indicates that it contains SNA) or ASCII (for all other frames).

The option you choose applies to all levels of all frames. The default is to show ASCII characters.

To select the type of interpretation:

1. Move to **Display\Hex**.
2. In the radio control to the right, move to the desired option and press Spacebar.

   ▶ ASCII characters
   EBCDIC characters
   Dynamic mode

Selecting ASCII Parity

You can also enable the **ASCII parity** option, which strips the 8th (high) bit from each byte. Since most protocols do not interpret the high bit, the default is **ASCII parity** disabled (x).

Function Keys Available During Display

While displaying the results of an interpretation in one—or all three—display views, the following function keys are available to manipulate the views.

F1 **Help.** Provides access to the Help system.

F2 **Set mark.** Marks the highlighted frame with the flag "M." The Sniffer analyzer uses this frame as the reference frame from which it

calculates relative time and cumulative bytes. (See "Flags Display Option" on page 7–40.)

F3 **Data display/Edit options.** Displays the data that passed the display filters in the formats you defined. After defining the display options (or at any other time when display was interrupted) press F3 **[Data display]** again to resume the display.

If the **Frame editing** option is enabled, this key toggles to **Edit options**, which allows you to edit frame content in the Hex view. (See "Using Hexadecimal View to Edit Frames," below.)

F4 **Zoom in/Zoom out.** Temporarily expands the active view to fill the entire window, which allows you to see more detail. To move to an enlarged version of any other open views, press the TAB key. To move to the previous view, press SHIFT-TAB.

Pressing F4 **[Zoom out]** a second time restores the arrangement of the open views.

F5 **Menus.** Displays the main menu.

F6 **Display options.** Displays the same set of display options as the main menu, as well as several additional options that allow you to search for frames, as described in "Searching for Frames" on page 7–55.

F7 **Previous frame**. Pressing F7 (or the CURSOR UP key) moves to the previous frame accepted by the filters, in all open views.

In the Summary view, the highlight moves to the preceding line (either the preceding frame or the preceding level of the current frame). In the Detail view and the Hex view, the current display is replaced by the display for the preceding frame.

F8 **Next frame.** Pressing F8 (or the CURSOR DOWN key) moves to the next line or the next frame, similar to the way F7 moves to the previous frame.

F9 **Select frame/Unselect frame**. Attaches the "S" flag to the highlighted frame. You can use this to select as many frames as you want and then save those frames to a file, as described in "Selected Frames Display Filter" on page 7–16.

Pressing F9 **[Unselect frame]** removes the flag from the highlighted frame.

F10 **New Capture/Stop capture.** Starts the capture process.

When capture is in progress, pressing F10 **[Stop capture]** again stops the capture. To ensure that the captured frames include the frame that interests you, set a trigger, as described in "Defining a Trigger to Stop Capture" on page 6–62.

Using Hexadecimal View to Edit Frames

The **Frame editing** option lets you edit the contents of a frame to change its size, content, or timing. This option is useful for development tasks such as writing protocol interpreters, where it allows you to simulate conditions for testing. It is also useful for inserting or deleting bytes in misaligned frames so that the DLC content may be decoded. By using the **Buffer mode** option in the **Traffic generator** function, you can transmit buffers you create with frame editing.

WARNING. If display filters are enabled and the frame being edited is changed so that it fails the filtering criteria, making either the Summary or Detail views active causes the frame to be filtered out. As long as the Hex view is active, the frame being edited is protected from any filters.

As you edit a frame, the Sniffer analyzer attempts to change the associated descriptions in the Summary and Detail views to match the edited content. Sometimes, however, it may not be able to do so, such as when the value of the edited frame depends on those of the previous frame, as in a session or connection-related protocol interpretation.

When you complete editing the frame, you can reinterpret the entire capture buffer so that any options or filters are applied to the edited frame. After reinterpretation, all views will contain the correct descriptions.

When editing frames, consider the following:

- In the Summary view, edited frames have an "E" flag, whether or not the **Flags** option is enabled. In the Detail view, the first line reads "This frame has been edited."
- As long as the Hex view is active, edited frames are not affected by any enabled display filters. This ensures that an edited frame is not eliminated from the display by a filter. When you reinterpret edited frames, however, or when you make the Summary or Detail views active, all filters and other settings are applied.
- You can use the Edit option **Delta time** (time between frames) to speed up or delay a transmission, which allows you to affect loads.

- You can choose the Edit option **Insert/Delete** to change the frame size. However, be careful not to exceed or go below the legal frame sizes for your particular network.
- You can use the Edit option **Overwrite** to change only existing frame data.
- On analyzers with an Ethernet-II adapter card, you can use the **Frame editing** option to create bad CRC frames.

Figure 7–35 shows the options associated with Frame editing.

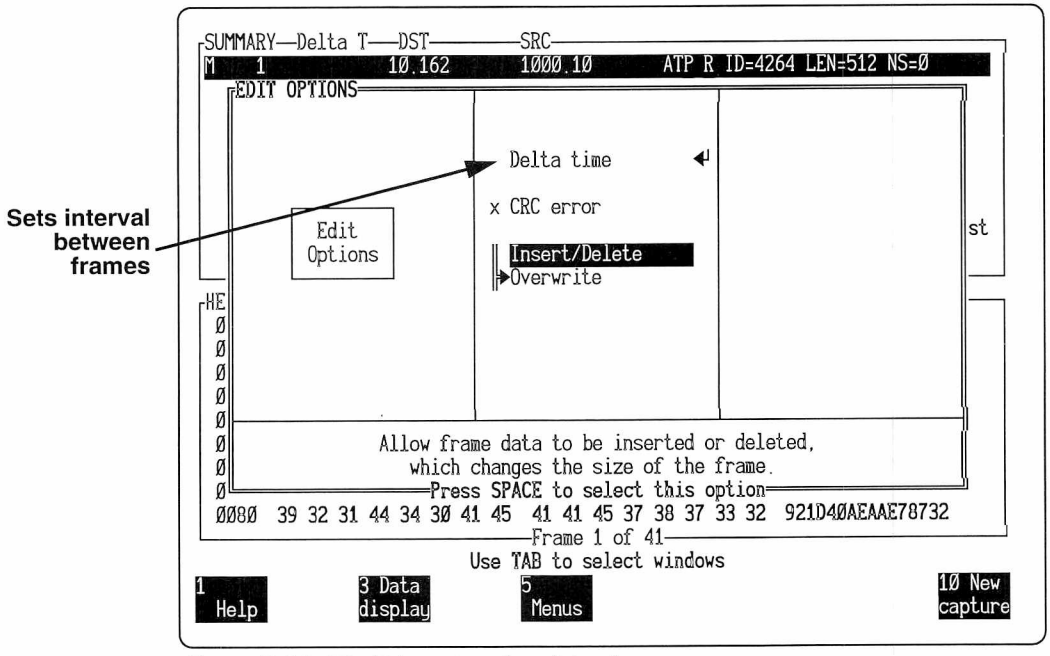

Sets interval between frames
SUMMARY—Delta T—DST—SRC
M 1 10.162 1000.10 ATP R ID=4264 LEN=512 NS=0
EDIT OPTIONS
Delta time
x CRC error
Edit Options
Insert/Delete
Overwrite
st
HE
Allow frame data to be inserted or deleted, which changes the size of the frame.
Press SPACE to select this option
0000 39 32 31 44 34 30 41 45 41 41 45 37 38 37 33 32 921D40AEAAE78732
Frame 1 of 41
Use TAB to select windows
1 Help
3 Data display
5 Menus
10 New capture

Figure 7–35. The Edit options for editing frames

To edit frames:

1. Move to **Display\Frame editing** and press Spacebar to enable (√) the option.
2. Move to **Display\Hex** and press Spacebar to enable the option.
3. Depending on what other information you want to display, enable the following options:

   √ Summary
   √ Detail
   √ Flags
   √ Delta time
4. Press F3 **[Data display]** and press TAB to make the Hex view active.

The cursor blinks on the first byte. If the cursor is a block (the default), whatever you type will overwrite the existing values. If the cursor is an underline, information you type will be inserted and pressing the DELETE key will delete existing information.

5. (Optional) Press F3 **[Edit options]** to determine the edit options. This includes **Delta time** and the edit mode.
   a. To change the interval between frames, move to **Delta time** and press ENTER. Enter the desired interframe delay (in milliseconds) in the dialog box.
   b. To change between the overwrite and insert modes, move to the desired edit mode and press Spacebar.

      Insert/Delete
      Overwrite

   c. To create a bad CRC frame (Ethernet-II only), move to **CRC error** and press Spacebar to enable (√) the option.
6. (Optional) Determine whether to edit the hex codes or the corresponding ASCII (or EBCDIC) characters. To toggle between the two modes, press F2 **[Edit text\Edit hex]**.
7. Press the Cursor keys to move to the Hex position you want to edit and type the desired characters. As you type, you can usually see that the corresponding text in the Summary and the Detail views changes.

   In the Summary view, the "E" flag appears in the far left column. This flag is *not* sent if you use the edited frame to generate traffic. In the Detail view, the first line identifies the frame as edited (for the transmitting station only).

To reinterpret edited frames:

1. If necessary, press F6 **[Display options]** to display the Display options menu.
2. Move to **Reinterpret** and press ENTER.

   In response, the analyzer reinterprets all frames, including those you edited, using any filters and other options you enabled.

Searching for Frames

You can always find a frame by scrolling though the Summary view. However, there are shortcuts that will locate the desired frame more quickly and conveniently. When searching for frames, you can specify the following criteria:

Frame number	Moves to the frame number you specify.
Text	Searches for text you specify, in either the Summary, Detail, or Hex views.

Pattern	Searches for a pattern you specify.
Mark	Moves to the reference frame, which you can specify with the "M" flag.
Trigger	Moves to the trigger frame, which is identified by the system with the "T" flag.

In the Summary view, you can also move to the last frame by pressing the END key. In the Detail view, this key moves to the last line for the current frame.

Figure 7–36 shows the search options in the Display Options menu, specifically those associated with the **Search for text** option.

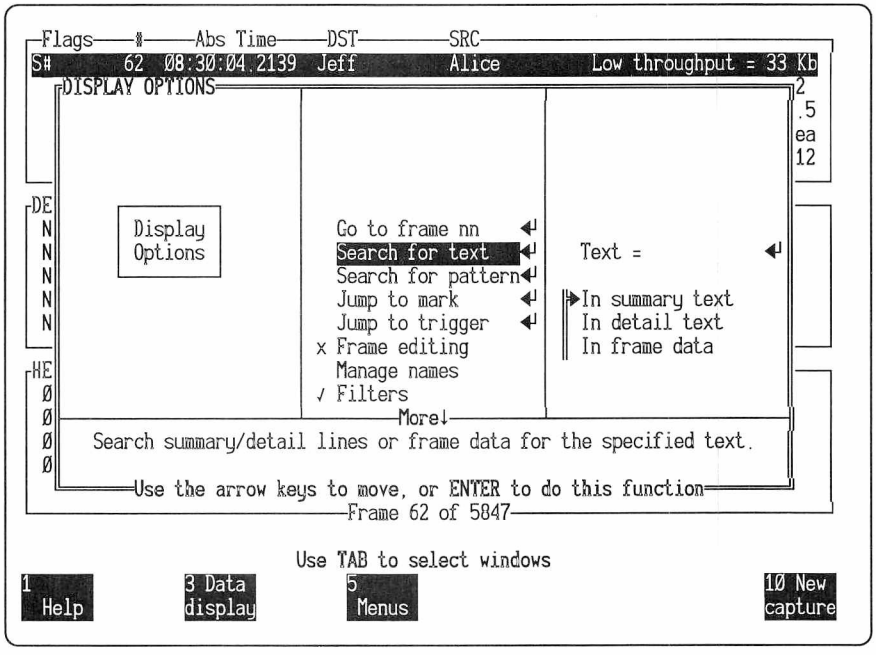


Figure 7–36. Text search options

Searching for a Frame Number

If you know the frame number, enter it as the search criterion.

To go to a frame number:

1. During display, press F6 **[Display options]**.
2. Move to **Go to frame nn** and press ENTER.

3. In the dialog box that appears, enter the desired frame number and press ENTER. You cannot specify a number larger than the number of frames in the capture buffer.

Searching for Text

You can also search the capture buffer for a frame that contains a particular text string. This text can either be a part of the data contained within the frames (when searching the frame data in the Hex view) or it can be a part of the analyzer's interpretation of the frames (when searching the Summary and Detail views).

The search starts with the frame that follows the highlighted frame and stops at the first match. If a match is not found, searching continues from the first frame in the capture buffer. If it still does not find a match, the analyzer displays "Match not found" and stops searching.

Figure 7–37 shows the options associated with searching for text.

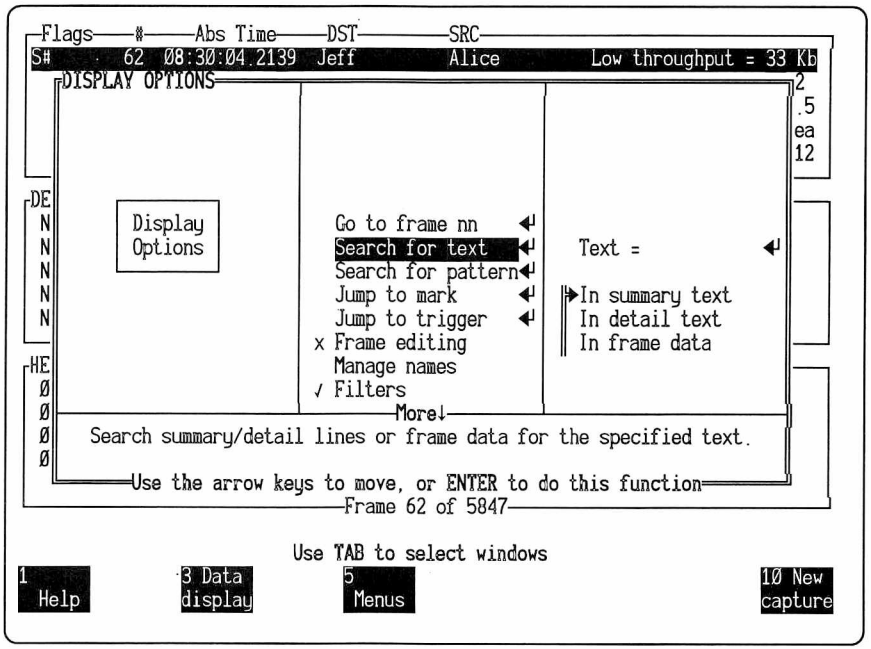


Figure 7–37. Searching the capture buffer for text

Figure 7–38 is an example of how to search captured frames for the phrase "Distance = 6" in the Detail view.

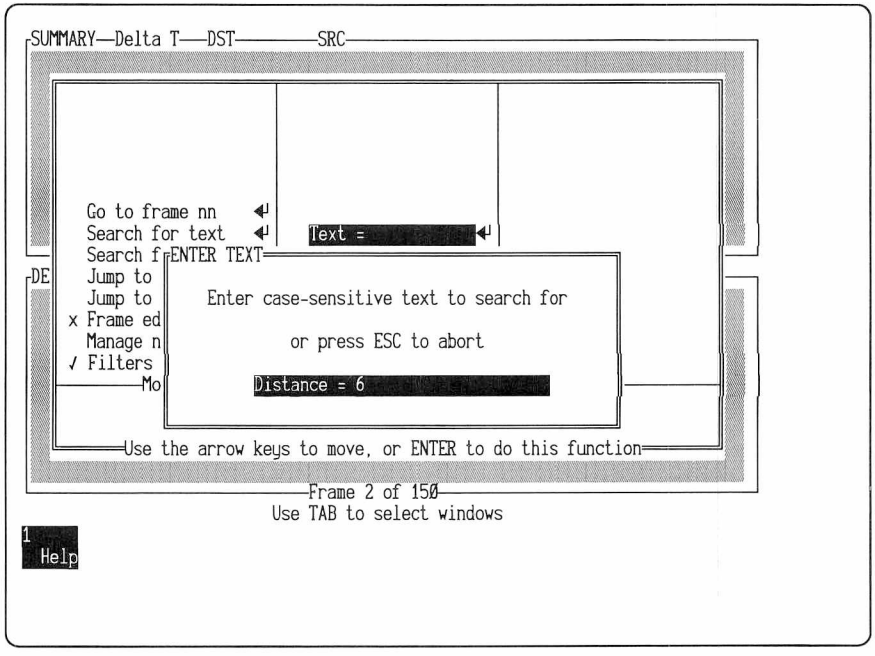


Figure 7–38. Entering text for which to search

To search for text:

1. During display, press F6 **[Display options]** to show the **Display options** menu.
2. Specify which view is to be searched. Move to the desired option and press Spacebar.

   ▶ In summary text (default)
   In detail text
   In frame data

   If you chose the **In frame data** option, you can also choose the type of text interpretation.

   ▶ ASCII (default)
   EBCDIC
3. Move to **Search for text** and then to **Text =**. Press ENTER.
4. In the dialog box that appears, type up to 31 characters. Because the search is case-sensitive, make sure you enter the letters exactly as they appear in the text.

You can continue searching the capture buffer for other matches that match the specified text.

To repeat a search for text:

1. Press F6 again for the Display Options menu.
2. Move to **Search for text** and press ENTER.
   The text dialog box appears, with the string you specified previously in the **Text =** field.
3. To search again for the same text, press ENTER. Otherwise, type new text and then press ENTER.

Searching for a Pattern

You can also search for frames that contain particular patterns.

As with a text search, a pattern search starts with the frame that follows the highlighted frame and stops at the first match. If the search reaches the last frame in the capture buffer without finding a match, searching continues from the first frame. If no matches are found, the analyzer displays "Match not found" and stops searching.

When the analyzer finds the specified pattern, it displays the message "Found at frame nn." If the Summary view is open, the analyzer highlights the match frame.

Figure 7–39 shows the options associated with searching for a pattern.

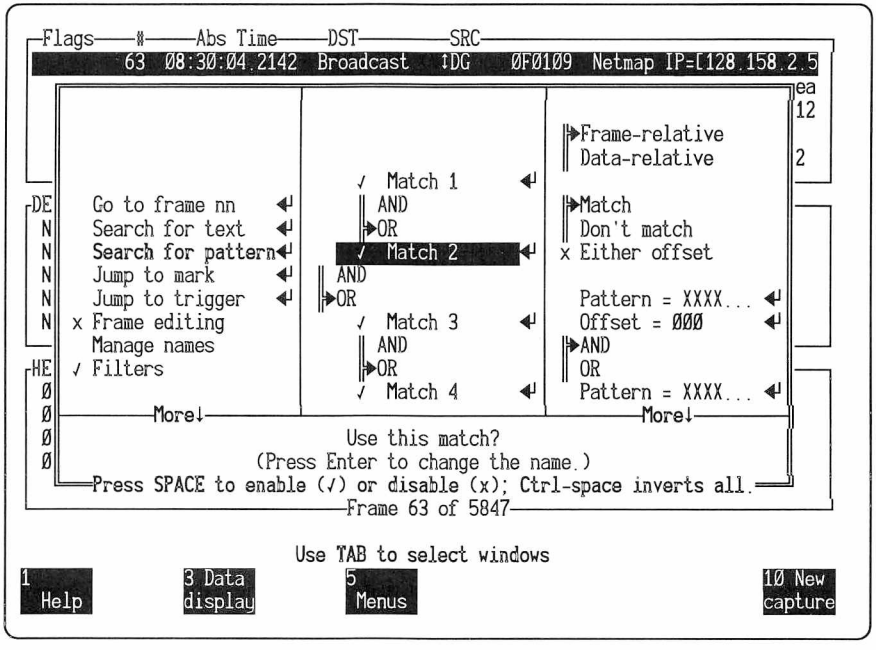


Figure 7–39. Searching the capture buffer for a pattern

To search the capture buffer for a pattern:

1. Press F6 [**Display options**] to show the **Display options** menu.
2. Move to **Search for Pattern** and then to the right to define up to four matches and the relationships to one another. (For more information about setting up patterns, see "Defining Complex Pattern Matches" on page 6–46.)
3. Return to **Search for Pattern** and press ENTER.

To repeat a search for a pattern:

1. Press F6 [**Display options**] again to return to the **Display options** menu.
2. To search for the same pattern, press ENTER. To specify a new pattern, follow the previous procedure, starting with step 2.

Jumping to the Marked Frame

You can jump to the reference (marked) frame, which is identified with the "M" flag. This frame is either the first frame in the capture buffer (default) or a frame you specify by pressing F2 [**Set mark**] when that frame is highlighted.

To jump to the marked frame:

1. Press F6 again to display the Display options menu.
2. Move to **Jump to mark** and press ENTER.

Jumping to the Trigger Frame

You can also jump to the trigger frame, which is identified with the "T" flag.

To jump to the trigger frame:

1. Press F6 again to display the **Display options** menu.
2. Move to **Jump to trigger** and press ENTER.

Printing and Importing Data

You can save, print, or import displayed frames, including frames you can see only by scrolling. (This manual calls printed or imported data "reports.")

For instructions on how to save data, see "Saving Captured Frames as Data (Trace) Files" on page 8–11. To prepare for printing or importing, you can define the following options:

- Range of included frames
- The destination, either a printer or file
- File format
- Page titles (if any)
- Page size

Figure 7–40 shows the options associated with printing and importing data.

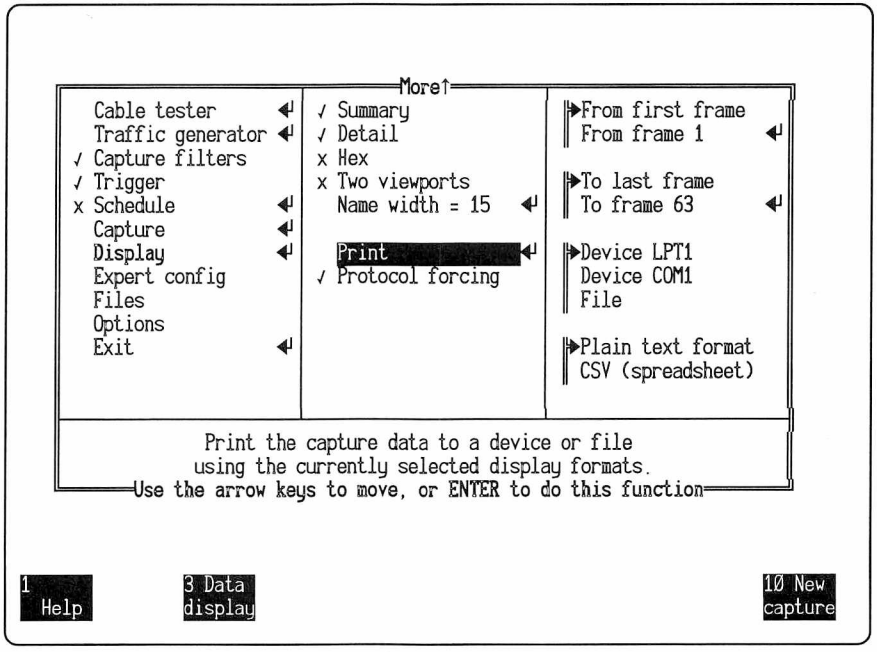


Figure 7–40. Printing and importing data

In general, printed or imported data shows the information on the screen, but without the restrictions of the small window. If both the Summary and the Detail views are open, the Summary data is printed first followed by the Detail data, with protocols in order from lowest to highest layer. Only those protocols enabled by the **Protocol** filter are included. When data is printed, there are no indications of highlighting or color.

The procedure that follows outlines the steps for printing and exporting. For more information about each of the options associated with the **Print** option, see the sections after the procedure.

To create a report:

1. Display the information you want to include.
   a. Set the display filters to exclude frames that do not interest you.
   b. Set the **Address level** filter to determine how source and destination are identified. (This setting affects the way source and destination are described, even if it does not alter which frames are displayed.)
   c. Enable (√) or disable (x) the **All layers** and **DLC addresses** options.
   d. Enable or disable the **Two-station format** option.
   e. Set the **Name width** field. If you widen this field, note that the analyzer does not fold the output lines, which makes it difficult to predict how long lines will be printed.
   f. Press F3 **[Data display]** to display the chosen views.
2. Define the range of frames in a report:
   a. Press F6 **[Display options]** to show the Display Options menu.
   b. Move to **Print** and then to the desired option. If you do not want to include the first and last frames, move to the **From frame xx** option and press ENTER.

      ▶ From first frame
      From frame *xx*

      ▶ To last frame
      From frame *xx*

   c. In the dialog box that appears, enter a frame number and press ENTER.
3. Define the destination by moving to the desired option and pressing Spacebar.

   ▶ Device LPT1
   Device COM1
   File

4. Define the file format. If you want to import the data, move to **Delimited format** and press Spacebar to enable (√) or disable (x) the option.

   If you enable the **Delimited format** option, disable the **Print page titles** option. Most applications that accept delimited format do not accept page titles.
5. Determine whether to include page titles. Move to **Print page titles** and press Spacebar to enable (√) or disable (x) the option.
6. Determine the page size. Move to the **Page size** option and press ENTER. In the dialog box that appears, enter a value between 5 and 99 as the desired page size.
7. Move to **Print** and press ENTER. Depending on the report destination you specified, the report is either printed on the chosen printer or saved as a file.

If you chose the **File** option, a dialog box appears. Enter the filename, using no more than eight characters. Do not include an extension; the Sniffer analyzer automatically attaches the extension .PRN for a file in the normal file format or .CSV (comma-separated values) for a file in the delimited format.

Defining the Range of Frames

Unless you specify otherwise, the analyzer includes frames starting with the reference (marked) frame through the last frame in the buffer. The reference frame is the first frame in the buffer, unless you marked another frame by pressing F2 **[Set mark]**.

You can also specify the frame numbers of the first and last frames you want to include in the report.

Defining the Destination: Printer or File

You can either print displayed data or save it to disk as a file. Figure 7–41 shows the first page of a report on an Ethernet network, which was taken from the Summary view displayed in the two-station format.

Report destination options include:

LPT1	A parallel printer attached to the LPT1 port.
COM1	A serial printer attached to the COM1 port.
File	A file that is saved to disk (a:\ or c:\).

```
Sniffer Network Analyzer data from 6-Nov-91 at 14:23:58, file C:\CAPTURE\B2.FDC, Page 1

SUMMARY  Delta T    From Syner 002080              From Syner 0020C0

M    1           FFFFFFFFFFFF    Syner 002080     SMT NIF Request from 8 port DAC
     2    0.0090 FFFFFFFFFFFF    Syner 0020C0     SMT NIF Request from 8 port DAC
     3    0.0106 SMT NIF Response from 8 port DAC
     4   29.9009 FFFFFFFFFFFF    Syner 002080     SMT NIF Request from 8 port DAC
     5    0.0078 FFFFFFFFFFFF    Syner 0020C0     SMT NIF Request from 8 port DAC
     6    0.0117 SMT NIF Response from 8 port DAC
     7   29.8628 FFFFFFFFFFFF    Syner 002080     SMT NIF Request from 8 port DAC
     8    0.0077 FFFFFFFFFFFF    Syner 0020C0     SMT NIF Request from 8 port DAC
     9    0.0116 SMT NIF Response from 8 port DAC
    10   29.8145 FFFFFFFFFFFF    Syner 002080     SMT NIF Request from 8 port DAC
    11    0.0078 FFFFFFFFFFFF    Syner 0020C0     SMT NIF Request from 8 port DAC
```

Figure 7–41. Portion of a printed report

Defining the File Format

You can define the format for data to be printed or exported. For printing, you should generally disable the **Delimited format** option. For importing, you can enable this option to format the data in the CSV format, which is widely used for importing data to spreadsheets.

NOTE: Although you can enable the **Delimited format** option when the Detail or Hex views are open, this format does not apply to the data from those views. Instead, the report will be in the standard printer format.

In delimited format, each character field is surrounded by double quotes and successive fields are separated by commas, as shown in Figure 7–42. The file's first line defines the fields. Each subsequent line is a *record* that contains the values for each field. Each line in the imported file corresponds to a row in the Summary view.

Whether the format shows a single line per frame or one line per protocol level depends on whether the **All layers** display option is enabled (see "All Layers Display Option" on page 7–36). As a result, the file will contain either one line per frame or one line per enabled protocol level.

If the Summary view shows multiple lines, fields that are the same for each line are shown only in the first line. For example, the frame number is shown only with the first of the protocols for that frame. However, in the corresponding delimited file, every line is filled, even when it is part of the same frame.

For examples of the normal and delimited formats, compare Figure 7–41 and Figure 7–42.

```
"Flags","Frame","Delta Time","Destination","Source","Protocol","Summary"
" ", 120, 5.4869,"15625.255 ","15625.220 ","DLC"," LAP type=DDP Short"
" ", 120, 5.4869,"15625.255 ","15625.220 ","DDP","D=15625.255 S=15625.220 Type=1 (RTMP data)"
" ", 120, 5.4869,"15625.255 ","15625.220 ","RTMP","R NET=1289 Routing entries=48"
" ", 123, 1.8765,"1045.20 ","1289.103 ","DLC"," LAP type=DDP Long"
" ", 123, 1.8765,"1045.20 ","1289.103 ","DDP","D=1045.20 S=1289.103 Type=3 (ATP)"
" ", 123, 1.8765,"1045.20 ","1289.103 ","ATP","C ID=2671 LEN=0"
" ", 123, 1.8765,"1045.20 ","1289.103 ","ASP","C OpenSess WSS=253 Version=0100"
" ", 126, 0.0222,"1289.103 ","1045.20 ","DLC"," LAP type=DDP Long"
" ", 126, 0.0222,"1289.103 ","1045.20 ","DDP","D=1289.103 S=1045.20 Type=3 (ATP)"
" ", 126, 0.0222,"1289.103 ","1045.20 ","ATP","R ID=2671 LEN=0 NS=0 "
" ", 126, 0.0222,"1289.103 ","1045.20 ","ASP","R OpenSess SSS=139 ID=49 ERR=0"
" ", 129, 0.0028,"1045.20 ","1289.103 ","DLC"," LAP type=DDP Long"
" ", 129, 0.0028,"1045.20 ","1289.103 ","DDP","D=1045.20 S=1289.103 Type=3 (ATP)"
" ", 129, 0.0028,"1045.20 ","1289.103 ","ATP","D ID=2671 "
" ", 132, 0.0033,"1045.20 ","1289.103 ","DLC"," LAP type=DDP Long"
" ", 132, 0.0033,"1045.20 ","1289.103 ","DDP","D=1045.20 S=1289.103 Type=3 (ATP)"
" ", 132, 0.0033,"1045.20 ","1289.103 ","ATP","C ID=2672 LEN=0"
" ", 132, 0.0033,"1045.20 ","1289.103 ","ASP","C Tickle ID=49"
" ", 135, 0.0031,"1289.103 ","1045.20 ","DLC"," LAP type=DDP Long"
" ", 135, 0.0031,"1289.103 ","1045.20 ","DDP","D=1289.103 S=1045.20 Type=3 (ATP)"
" ", 135, 0.0031,"1289.103 ","1045.20 ","ATP","C ID=16531 LEN=0"
" ", 135, 0.0031,"1289.103 ","1045.20 ","ASP","C Tickle ID=49"
" ", 138, 0.0044,"1045.20 ","1289.103 ","DLC"," LAP type=DDP Long"
" ", 138, 0.0044,"1045.20 ","1289.103 ","DDP","D=1045.20 S=1289.103 Type=3 (ATP)"
" ", 138, 0.0044,"1045.20 ","1289.103 ","ATP","C ID=2673 LEN=46"
" ", 138, 0.0044,"1045.20 ","1289.103 ","ASP","C Command ID=49 SEQ=0 LEN=46"
" ", 138, 0.0044,"1045.20 ","1289.103 ","AFP","C Login AFPVersion 1.1"
" ", 141, 0.2662,"1289.103 ","1045.20 ","DLC"," LAP type=DDP Long"
" ", 141, 0.2662,"1289.103 ","1045.20 ","DDP","D=1289.103 S=1045.20 Type=3 (ATP)"
" ", 141, 0.2662,"1289.103 ","1045.20 ","ATP","R ID=2673 LEN=0 NS=0 (Last)"
" ", 141, 0.2662,"1289.103 ","1045.20 ","ASP","R Command RESULT=-5019 LEN=0"
" ", 141, 0.2662,"1289.103 ","1045.20 ","AFP","R Error=ParamErr "
" ", 144, 0.0028,"1045.20 ","1289.103 ","DLC"," LAP type=DDP Long"
" ", 144, 0.0028,"1045.20 ","1289.103 ","DDP","D=1045.20 S=1289.103 Type=3 (ATP)"
" ", 144, 0.0028,"1045.20 ","1289.103 ","ATP","D ID=2673 "
" ", 147, 0.0035,"1045.20 ","1289.103 ","DLC"," LAP type=DDP Long"
" ", 147, 0.0035,"1045.20 ","1289.103 ","DDP","D=1045.20 S=1289.103 Type=3 (ATP)"
" ", 147, 0.0035,"1045.20 ","1289.103 ","ATP","C ID=2674 LEN=0"
" ", 147, 0.0035,"1045.20 ","1289.103 ","ASP","C CloseSess ID=49"
" ", 150, 0.0194,"1289.103 ","1045.20 ","DLC"," LAP type=DDP Long"
" ", 150, 0.0194,"1289.103 ","1045.20 ","DDP","D=1289.103 S=1045.20 Type=3 (ATP)"
" ", 150, 0.0194,"1289.103 ","1045.20 ","ATP","R ID=2674 LEN=0 NS=0 "
" ", 150, 0.0194,"1289.103 ","1045.20 ","ASP","R CloseSess "
```

Figure 7–42. Delimited format (all levels)

Choosing Page Titles

You can choose whether to include page titles for each page. Page titles specify the date and time the data was recorded, the network name (for a "live" capture) or the name of the file (for a capture from a file), and the page number. There are two blank lines between the heading and the start of the data.

If you enable the **Print page titles** option, you also cause explicit page breaks because the analyzer includes a form-feed character after the last non-blank line of each page. This option is automatically disabled if you enable the **Delimited format** option, because most applications that accept the delimited format do not accept page titles.

Choosing Page Size

You can also set the page size, which determines the number of lines per page. The default is 50 lines. Depending on whether you enabled the **Print page titles** option, this setting would result in either 50 printed lines or, with a page title, two blank lines and 47 lines of data. Since each page break is indicated by an explicit form feed, there is no separate setting for the physical length of the paper.

Background Information: Protocol Interpretation

This section provides background information to help you understand the analyzer's displays.

Transmission of 6-Byte DLC Addresses

At the DLC level, each address uniquely identifies a station's network interface card.

- The first three bytes of the address are an IEEE-assigned code that identifies the adapter card's manufacturer.
- The last three bytes contain an unique identifier for each network interface card.

Bits on the Wire vs. Bits in Memory

Different network technologies have different rules for converting bits "on the wire" to bits in computer memory. Some systems transmit each byte high-order bit first and some transmit low-order bit first. For example, suppose a byte of computer memory contains the value 87. In memory, that consists of the following bits:

```
1 Ø Ø Ø  Ø 1 1 1
  8        7
```

- For FDDI or 802.5 ring cable, each byte is transmitted with the high-order bits first: 1 0 0 0 0 1 1 1.
- For Ethernet,each byte is transmitted with the low-order bit first: 1 1 1 0 0 0 0 1.

Ordinarily, these different ways of transmitting are invisible to users or programs. The adapter card translates between bits on the wire and bits in computer memory. You see only bytes in memory before they are sent or after they are received, but never while they are in transit. When an Ethernet card receives the sequence 1 1 1 0 0 0 0 1, it turns that sequence into hex 87, and the receiving station has the same value as the sender. Since (at the DLC level) sender and receiver must be on the same network and must use compatible equipment, a byte in the sender's memory results in the same byte in the receiver's memory.

Consequence of the IEEE standard

When the IEEE assigned codes to the various manufacturers, it specified the sequence in which bits are transmitted on the wire. It did not specify what the sender or receiver would see in memory. For example, Network General Corporation was assigned a particular sequence of bits. To transmit that sequence on token ring, an analyzer has in its memory the bytes 00 00 A6. But to transmit that same sequence on Ethernet, the Sniffer's memory must contain the bytes 00 00 65 because A6, with the bits of each byte reversed, is 65.

So, to comply with the IEEE standard, a given manufacturer ID should translate to one number for Ethernet (or any other network using low-order bit -first), and to a different number for token ring. (Token ring and FDDI are the only topologies that use the high-order bit first.) Consequently, the Analyzer has one manufacturers' code table for token ring/FDDI and a different table for other networks.

NOTE: Some manufacturers do not follow the IEEE standard. They use the same value in memory for both network types.

Protocol Interpretation

The analyzer gets its ability to interpret protocols from several sources. Interpretation for protocols at the lowest level is included in the software that supports the type of network that the analyzer monitors. Interpreters for higher-level protocols are available in suites.

The interpreters from these different sources are linked to the analyzer's executable file when it is built. Each protocol interpreter registers its presence and facilities with the analyzer, which permits each interpreter to be represented in the appropriate menus and displays. In the Detail view, in the left column of every line, each interpreter shows the abbreviation of the protocol it is decoding.

While a common registration and display procedure applies to all of the interpreters, the interpreters are independent, just as the protocols are independent. Within each protocol, the fields displayed are those that make sense within the context of the protocol.

Bit-Level Interpretation

A protocol may record binary attributes as individual bits in a byte. For these protcols, the interpreters often explode each byte to show its eight bits separately. Figure 7–43 illustrates the interpretation of hex 1F at a particular position in the Banyan VINES protocol called VIP. Figure 7–44 shows an interpretation of the sequence 6B 80 00 from an IBM SNA header. This sort of decoding interprets not only the meaning of each bit set at a certain position, but also the meaning of each bit *not* set (that is, each

0). Bit-level interpretation is included in almost all protocols; however, in X Window it is not universally shown, because the number of possible bit-encodings is extremely large.

```
VIP: Transport control = 1F
VIP: ØØ.. .... = Unused
VIP: ..Ø. .... = Do not return metric notification packet
VIP: ...1 .... = Return exception notification packet
VIP: .... 1111 = Hop count remaining (15)
```

Figure 7–43. Bit-by-bit interpretation of a byte of VINES internet protocol

```
SNA: ----- SNA Request Header (RH) -----
SNA:
SNA: RH byte Ø = 6B
SNA: Ø... .... = Command
SNA: .11. .... = RU category is session control
SNA: .... 1... = Format indicator
SNA: .... .Ø.. = Sense data are not included
SNA: .... ..11 = Only RU in chain
SNA: RH byte 1 = 8Ø
SNA: 1.ØØ .... = Definite response requested
SNA: .... ..Ø. = Response bypasses TC queues
SNA: .... ...Ø = Pacing indicator
SNA: RH byte 2 = ØØ
SNA: Ø... .... = Begin bracket indicator
SNA: .Ø.. .... = End bracket indicator
SNA: .... ...Ø = Conditional end bracket indicator
SNA: ..Ø. .... = Change direction indicator
SNA: .... Ø... = Character code selection indicator
SNA: .... .Ø.. = Enciphered data indicator
SNA: .... ..Ø. = Padded data indicator
```

Figure 7–44. Bit-by-bit interpretation of three SNA bytes on token ring

Alternate Displays for ASN.1-Encoded Protocols

ISO protocols at the presentation and application levels can be interpreted in two modes. Each is written so that it conforms to a general syntax specified in ASN.1 (Abstract Syntax Notation 1, ISO 8825). The individual protocols then assign meanings to the components identified by the ASN.1 syntax. To accommodate this dual level of interpretation, the ISO protocol interpreter suite gives you the option to interpret frames in these layers in either of two ways:

Syntactic	The analyzer labels the ASN.1 components within each frame.
Semantic	The analyzer interprets what the various ASN.1 statements mean, according to the rules of the particular protocol in which the ASN.1 statements occur.

When you select interpretation at the X.400 level, you get the semantic interpretation. To see ASN.1 interpretation, disable X.400 in the protocol display filter.

Figure 7–45 shows the same fragment of an X.400 frame interpreted first for ASN.1 syntax and then for its content as part of a P1 message envelope.

```
X.400: -- X.400 Message Transfer Protocol (P2) --
X.400:
X.400: 1.1 Context-Specific Constructed [0], Length=Indefinite
X.400: 2.1 SET [of], Length=Indefinite
X.400: 3.1 Application Constructed [4], Length=Indefinite
X.400: 4.1 Application Constructed [3], Length=Indefinite
X.400: 5.1 Application Constructed [1], Length=Indefinite
X.400: 6.1 PrintableString, Length=2, Value = "US"
X.400: 5.2 Application Constructed [2], Length=Indefinite
X.400: 6.1 PrintableString, Length=7, Value = "ATTMAIL"
X.400: 5.3 PrintableString, Length=5, Value = "KANJI"
X.400: 4.2 IA5String, Length=19, Value = "VAX 880726 14:53:53"
X.400: 3.2 Application Constructed [0], Length=Indefinite
X.400: 4.1 SEQUENCE [of], Length=Indefinite
X.400: 5.1 Application Constructed [1], Length=Indefinite
X.400: 6.1 PrintableString, Length=2, Value = "US"
X.400: 5.2 Application Constructed [2], Length=Indefinite
X.400: 6.1 PrintableString, Length=7, Value = "ATTMAIL"
X.400: 5.3 Context-Specific Constructed [2], Length=Indefinite
X.400: 6.1 PrintableString, Length=5, Value = "KANJI"
X.400: 5.4 Context-Specific Primitive [3], Length=3, Data = "VAX"
X.400: 5.5 Context-Specific Constructed [5], Length=Indefinite
X.400: 6.1 Context-Specific Primitive [0], Length=7, Data = "FRASIER"
X.400: 6.2 Context-Specific Primitive [1], Length=5, Data = "ALLEN"
X.400: 6.3 Context-Specific Primitive [2], Length=1, Data = "D"
X.400: 3.3 Application Constructed [5], Length=Indefinite
X.400: 4.1 Context-Specific Primitive [0], Length=3, Data = "<04A000>"
X.400: 3.4 Application Primitive [6], Length=1, Data = "<02>"
X.400: 3.5 Application Primitive [10], Length=15, Data = "880726 14:53:53"
X.400: 3.6 Application Primitive [7], Length=1, Data = "<02>"
X.400: 3.7 Application Primitive [8], Length=2, Data = "<03C0>"
X.400: 3.8 Context-Specific Constructed [2], Length=Indefinite
X.400: 4.1 SET [of], Length=Indefinite
X.400: 5.1 Application Constructed [0], Length=Indefinite
X.400: 6.1 SEQUENCE [of], Length=Indefinite
X.400: 7.1 Application Constructed [1], Length=Indefinite
X.400: 8.1 PrintableString, Length=2, Value = "US"
X.400: 7.2 Application Constructed [2], Length=Indefinite
X.400: 8.1 PrintableString, Length=7, Value = "ATTMAIL"
X.400: 7.3 Context-Specific Constructed [2], Length=Indefinite
X.400: 8.1 PrintableString, Length=5, Value = "kanji"
X.400: 7.4 Context-Specific Primitive [3], Length=3, Data = "sun"
X.400: 7.5 Context-Specific Constructed [5], Length=Indefinite
X.400: 8.1 Context-Specific Primitive [0], Length=8, Data = "danville"
X.400: 8.2 Context-Specific Primitive [1], Length=7, Data = "roberta"
X.400: 5.2 Context-Specific Primitive [0], Length=1, Data = "<01>"
X.400: 5.3 Context-Specific Primitive [1], Length=2, Data = "<00A8>"
X.400: 4.2 SET [of], Length=Indefinite
X.400: 5.1 Application Constructed [0], Length=Indefinite
X.400: 6.1 SEQUENCE [of], Length=Indefinite
X.400: 7.1 Application Constructed [1], Length=Indefinite
X.400: 8.1 PrintableString, Length=2, Value = "US"
X.400: 7.2 Application Constructed [2], Length=Indefinite
X.400: 8.1 PrintableString, Length=7, Value = "ATTMAIL"
X.400: 7.3 Context-Specific Constructed [2], Length=Indefinite
X.400: 8.1 PrintableString, Length=5, Value = "kanji"
X.400: 7.4 Context-Specific Primitive [3], Length=3, Data = "sun"
X.400: 7.5 Context-Specific Constructed [5], Length=Indefinite
X.400: 8.1 Context-Specific Primitive [0], Length=7, Data = "frasier"
X.400: 8.2 Context-Specific Primitive [1], Length=5, Data = "allen"
X.400: 5.2 Context-Specific Primitive [0], Length=1, Data = "<02>"
X.400: 5.3 Context-Specific Primitive [1], Length=2, Data = "<00D0>"
X.400: 3.9 Application Constructed [9], Length=Indefinite
X.400: 4.1 SEQUENCE [of], Length=Indefinite
X.400: 5.1 Application Constructed [3], Length=Indefinite
X.400: 6.1 Application Constructed [1], Length=Indefinite
X.400: 7.1 PrintableString, Length=2, Value = "US"
X.400: 6.2 Application Constructed [2], Length=Indefinite
X.400: 7.1 PrintableString, Length=7, Value = "ATTMAIL"
X.400: 6.3 PrintableString, Length=5, Value = "KANJI"
X.400: 5.2 SET [of], Length=Indefinite
X.400: 6.1 Context-Specific Primitive [0], Length=17, Data = "880726145358-0700"
X.400: 6.2 Context-Specific Primitive [2], Length=1, Data = "<00>"
X.400: 3.10 Application Constructed [30], Length=Indefinite
X.400: 4.1 SEQUENCE [of], Length=Indefinite
X.400: 5.1 PrintableString, Length=3, Value = "VAX"
X.400: 5.2 SET [of], Length=Indefinite
X.400: 6.1 Context-Specific Primitive [0], Length=17, Data = "880726145358-0700"
X.400: 6.2 Context-Specific Primitive [2], Length=1, Data = "<00>"
X.400: 2.2 Constructed OCTET STRING, Length=Indefinite
X.400: 3.1 OCTET STRING, Length=2048, Value =
             "<A080>1<80>k<80>`<80>0<80>a<801302>US<0000>..."
X.400: 3.2 OCTET STRING, Length=85, Value =
           "<0000000000000000000000000000000000000000000000000000>
X.400:
```

```
X.400: -- X.400 Message Transfer Protocol (P1) --
X.400:
X.400: MPDU type = User (length = indefinite)
X.400: Envelope:
X.400: MPDU identifier:
            /C=US/ADMD=ATTMAIL/PRMD=KANJI/, VAX 880726 14:53:53
X.400: Originator: /C=US/ADMD=ATTMAIL/PRMD=KANJI/O=VAX/PN=FRASIER.ALLEN.D/
X.400: Original encoded information types:
X.400: Basic information type = A000
X.400: 1... .... .... .... = Undefined
X.400: .0.. .... .... .... = No tLX
X.400: ..1. .... .... .... = IA5Text
X.400: ...0 .... .... .... = No g3Fax
X.400: .... 0... .... .... = No tIF0
X.400: .... .0.. .... .... = No tTX
X.400: .... ..0. .... .... = No videotex
X.400: .... ...0 .... .... = No voice
X.400: .... .... 0... .... = No sFD
X.400: .... .... .0.. .... = No tIF1
X.400: Content type = 2 (P2)
X.400: UA content id = 880726 14:53:53
X.400: Priority = 2 (Urgent)
X.400: Per message flag = C0
X.400: 1... .... = Disclose recipients
X.400: .1.. .... = Conversion prohibited
X.400: ..0. .... = No alternate recipient allowed
X.400: ...0 .... = No content return request
X.400: Recipient info:
X.400: Recipient: /C=US/ADMD=ATTMAIL/PRMD=kanji/O=sun/PN=danville.roberta/
X.400: Extension identifier = 1
X.400: Per recipient flag = A8
X.400: 1... .... = responsibility flag on
X.400: .0.1 .... = basic report request
X.400: ...0 1... = basic user report request
X.400: Recipient info:
X.400: Recipient: /C=US/ADMD=ATTMAIL/PRMD=kanji/O=sun/PN=frasier.allen/
X.400: Extension identifier = 2
X.400: Per recipient flag = D0
X.400: 1... .... = responsibility flag on
X.400: .10. .... = confirmed report request
X.400: ...1 0... = confirmed user report request
X.400: Trace information:
X.400: Global domain identifier: /C=US/ADMD=ATTMAIL/PRMD=KANJI/
X.400: Arrival = 26 Jul 1988 14:53:58-0700
X.400: Action = 0 (Relayed)
X.400: Internal trace info:
X.400: MTA name = VAX
X.400: Arrival = 26 Jul 1988 14:53:58-0700
X.400: Action = 0 (Relayed)
X.400:
```

Figure 7–45. Bit-by-bit interpretation of three SNA bytes on token ring

Token Ring and FDDI Trailer Byte

As each frame circulates on the token ring, it has one extra "trailer" byte at the end. The trailer checks the frame's validity. It usually is not considered part of the frame and it does not appear in the Hex view. However, the Detail view reports the status of two indicators in the trailer: the address recognized bits and the frame copied bits. These bits are visible in Figure 7–46 as part of the Detail view's DLC report.

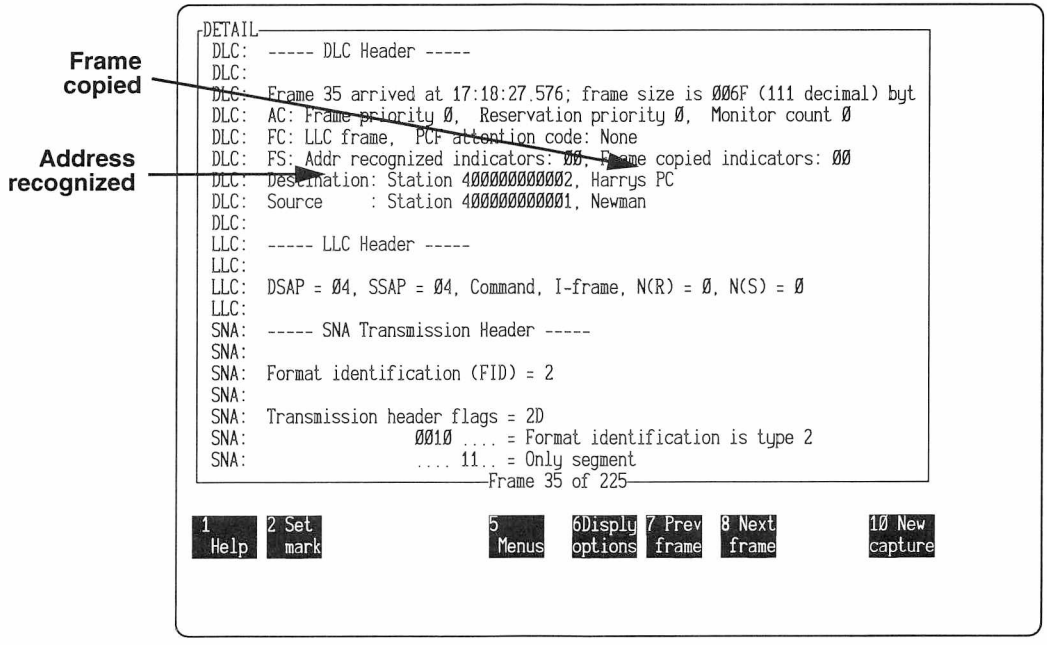

Frame copied
Address recognized
DETAIL
DLC: ----- DLC Header -----
DLC:
DLC: Frame 35 arrived at 17:18:27.576; frame size is 006F (111 decimal) byt
DLC: AC: Frame priority 0, Reservation priority 0, Monitor count 0
DLC: FC: LLC frame, PCF attention code: None
DLC: FS: Addr recognized indicators: 00, Frame copied indicators: 00
DLC: Destination: Station 400000000002, Harrys PC
DLC: Source : Station 400000000001, Newman
DLC:
LLC: ----- LLC Header -----
LLC:
LLC: DSAP = 04, SSAP = 04, Command, I-frame, N(R) = 0, N(S) = 0
LLC:
SNA: ----- SNA Transmission Header -----
SNA:
SNA: Format identification (FID) = 2
SNA:
SNA: Transmission header flags = 2D
SNA: 0010 .... = Format identification is type 2
SNA: .... 11.. = Only segment
Frame 35 of 225
1 Help
2 Set mark
5 Menus
6Disply options
7 Prev frame
8 Next frame
10 New capture

Figure 7–46. Detail view showing token ring "address recognized" and "frame copied" bits

When a station recognizes itself in the frame's destination, it sets the *address recognized* bits. If those bits are on when the frame reaches you, at least one station upstream from you has recognized itself as a recipient. (A frame sent to a functional address may have any number of recipients.)

When a station retains a copy of the frame, it sets the *frame copied* bits. Normally, a recipient both recognizes and records the frame, and sets both bits.

The values you see for *address recognized* and *frame copied* depend on where you are located. If a frame reaches you with *address recognized* bits already set, the frame must have reached the recipient before it reached you. When you are looking for problems at a particular portion of the ring, you may want to capture from different positions. The *address recognized* bits show your position in the ring sequence. To verify that a station has accepted frames addressed to it, you must be upstream from the sender and downstream from the recipient. (That is, you must not be between the sender and recipient in ring order.)

Managing Names and Working with Files

8

Managing Names and Working with Files

Overview

This chapter describes how to manage the information in the Sniffer Network Analyzer's name table and how to manage files that contain either captured frames or the various analyzer options and parameters you defined. It includes these topics:

- Managing the name table to include station names in the displays.
- Saving captured frames to data files, which you can use to load the capture buffer or when you use the **Traffic generator** feature.
- Saving the combination of options you define to the startup file or to setup files. The options in the startup file are automatically applied at system startup. You can apply the options in the setup files at any time.

Managing Names

To make its displays more readable, the analyzer displays the names associated with captured addresses. To find the names that correspond to the addresses, the analyzer refers to its name table, contained in the file STARTUP.*xx*D.

The name table is stored in expanded memory; it can contain up to 8000 pairs of addresses and names. To associate names with addresses, you can:

- Manually edit the name table
- Use external files to add names to addresses
- Use a feature that automatically adds system-assigned names to higher-level addresses

NOTE: You can increase the number of addresses in the name table to a maximum of 8000 by resetting the value for the associated parameter. For instructions, refer to "Editing the Startup Parameters" on page 11–22.

Once the name table contains the addresses and names you need, you can save it so it is used automatically the next time you start up the Sniffer analyzer. The sections that follow explain these options in more detail.

Figure 8–1 shows the menu options associated with managing the name table.

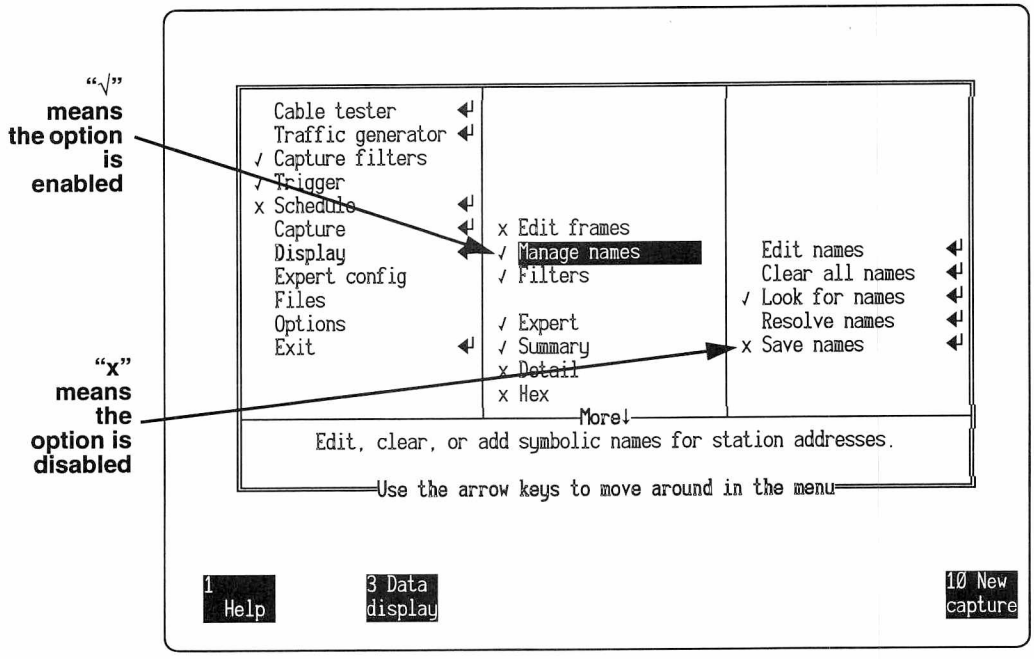


Figure 8–1. Managing the name table

About the Name Table

When you start the analyzer, the name table loads from the startup file and becomes the working name table.

The name table contains three columns, shown in Figure 8–2:

Address layer — The protocol in which the address can occur.

Station address — The byte sequence of the numeric station address.

Symbolic name — The name assigned to the address. If you do not assign a name to the address, this column is blank.

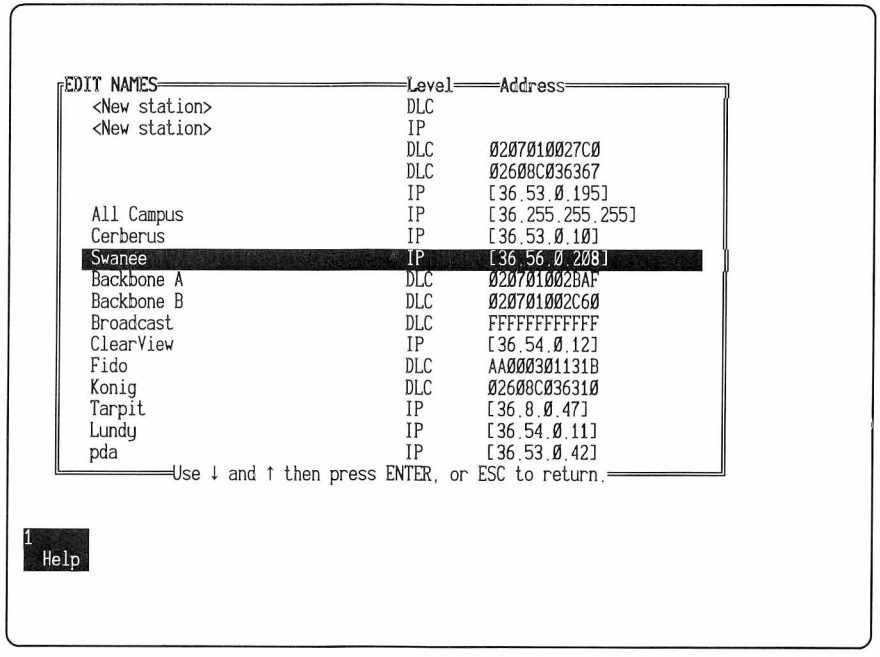


Figure 8–2. Sample working name table

A station address never exists alone; it is always paired with a specific protocol. A symbolic name refers to a protocol/address pair.

How the Analyzer Builds the Name Table

The analyzer builds and uses the name table this way:

Initialization — When the analyzer launches, it initializes the working name table with names and addresses in the file STARTUP.*xx*D. It also inserts its own address and assigns itself the name "This Sniffer," even when the saved table previously assigned it a different name.

Capture — During capture, the capture views show the station names (if they exist in the name table) or the station addresses.

First display — The first time you display interpreted data after a new capture, the analyzer scans the frames in the buffer for new addresses and enters them in the working name table with blank names.

Display — During display, the analyzer checks its name table for the address of each frame that appears in the Summary or Detail view. If it finds unnamed addresses, it adds them to the name table, up to 50 for each address level.

Editing — You can edit the working name table during capture or display. This includes adding new addresses, naming addresses, editing existing names, or deleting names and addresses.

Taking Advantage of the Automatic Address Scan

The first time you display captured frames after a new capture, the analyzer scans the capture buffer for addresses, including all address layers. During its scan for new addresses, the analyzer stops adding addresses when the table is full (default is 2000 addresses, possible maximum is 8000). It never adds more than 500 addresses at any level, even when there is room.

When the analyzer finds a new address, it adds that address to the top of the working name table, with a blank name field. Once an address exists in the name table you can assign it a name. (You can also add the address and the name manually.)

If you want to save new addresses, assign them a name. Unnamed addresses are purged when you exit the analyzer.

Assigning Names to Addresses

These options allow you to assign names to addresses.

Edit names — You can manually enter a name for each unnamed address.

Resolve names — The analyzer searches a file that contains a previously saved name table for any named DLC addresses that match the unnamed addresses in the working name table. If it finds these addresses, it copies the names from the file to the working name table.

Look for names — Certain protocols allow stations to exchange tables of higher-level addresses and associated names. This option scans the capture buffer for such messages and adds such pairs to the working name table.

Manually Editing the Name Table

The easiest way to manually edit the name table is to start a capture and let the analyzer compile a list of addresses automatically, then assign names to those addresses manually.

To edit the working name table:

1. Before you open the name table, compile a list of the addresses.
   a. Press F10 **[Start capture]** to capture frames (either live from the network or from a saved file). Press F10 **[Stop capture]** to stop the capture.
   b. Move to **Display** and press ENTER (or press F3).
2. Press F6 **[Display options]**.
3. Move to **Manage names\Edit names** and press ENTER to display the current name table.

   In this table (Figure 8–3), each name consists of a protocol layer and an address. For example, the name *Fido* is associated with the DLC layer and address AA0003 01131B. The name *Tarpit* is associated with the IP layer and address [36.8.0.47]. The DLC layer is always present.

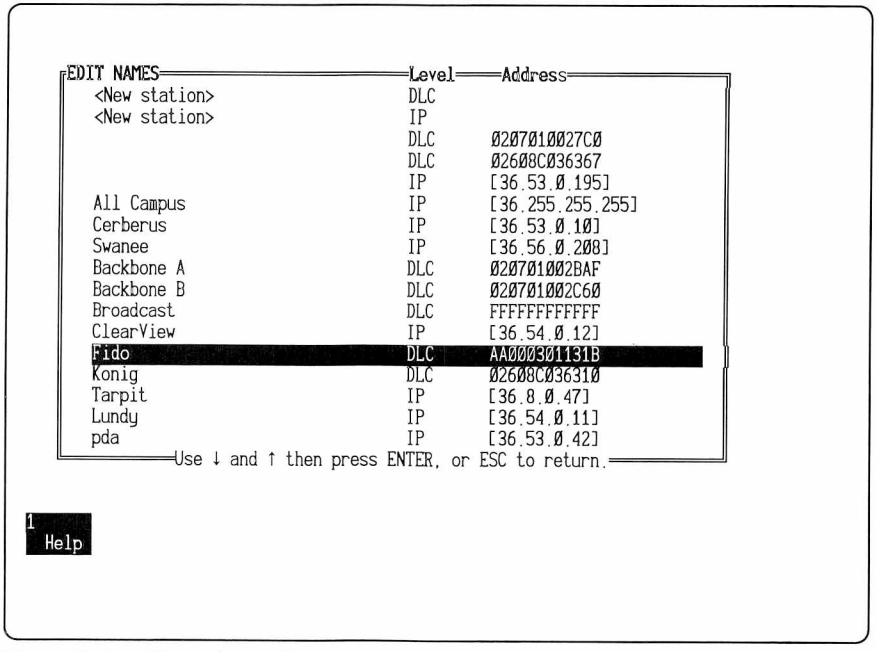


Figure 8–3. Editing the working name table

4. To edit an existing name, move to the item you want to change and press ENTER. In the dialog box that appears, enter the new name (Figure 8–4).

NOTE: To move to a name, enter the first few characters of the name. For example, you can type ed to get to the first name that starts with ed.To go to a new name before you press ENTER, press BACKSPACE once for each character you have entered, then enter the first few characters of the new name.

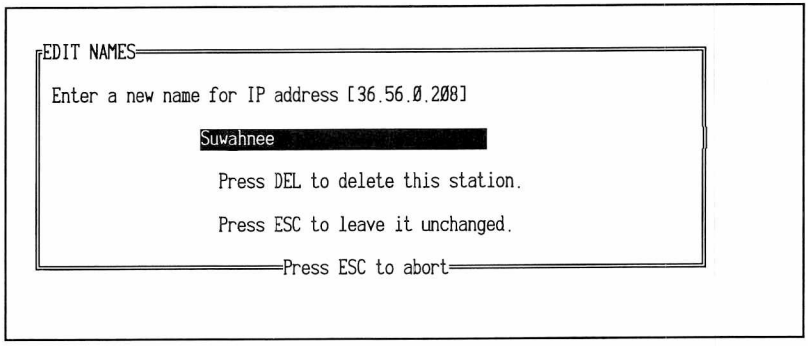

EDIT NAMES
Enter a new name for IP address [36.56.0.208]
Suwahnee
Press DEL to delete this station.
Press ESC to leave it unchanged.
Press ESC to abort

Figure 8–4. Changing an existing name

5. To add a name to an unnamed address, move to that address near the top of the list and press ENTER. In the dialog box that appears, enter the desired name.
6. To add an address that is not in the list, move to the top of the list to the line **<new station>** that has the appropriate protocol layer. Press ENTER.

   Each **<new station>** line is identified by its layer. There is always a line for the DLC layer. In addition, there is a line for each layer enabled in the **Address level** filter.

   In the dialog box that appears, enter the address (Figure 8–5).

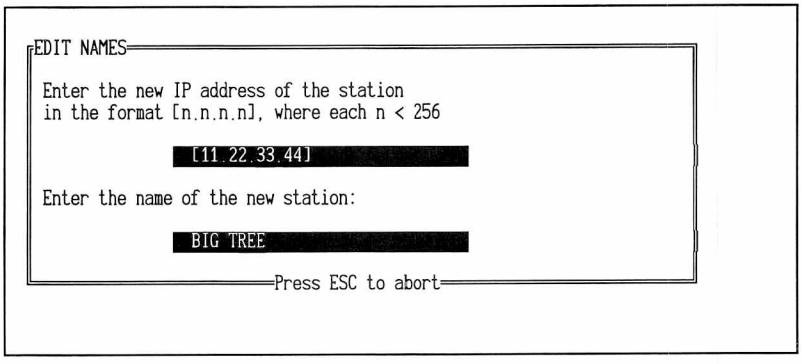

EDIT NAMES
Enter the new IP address of the station
in the format [n.n.n.n], where each n < 256
[11.22.33.44]
Enter the name of the new station:
BIG TREE
Press ESC to abort

Figure 8–5. Entering a station's name and address

IMPORTANT: When you use the **Edit Names** option to edit the name table, only the working name table is affected. If the **Save names** option is enabled (the default), the analyzer updates the startup file with new address and name pairs. If the option is disabled, you can save manually by moving to **Save Names** and pressing ENTER.

Using Name Files to Resolve Names

Instead of manually editing the name table, you can use name files that contain name tables (saved under different names) that identify unnamed DLC addresses. These files have the same format as the file STARTUP.*xx*D.

You can create name files by copying and renaming the current version of the STARTUP.*xx*D file or by creating them with a text editor. These files must have the identifying extension .*xx*D and they must be in the same format as the STARTUP.*xx*D file. (The requirements for name files are described in Chapter 11, "The Analyzer's File System.")

How the Resolve Names Option Works

After scanning the capture buffer, the Sniffer analyzer adds to the working name table all addresses that are not named, at all address levels. This results in a list of unnamed stations, including unnamed stations in the capture buffer and unnamed stations in the name table.

For each address in this list of unnamed stations, the analyzer searches the name file you select. When it finds a name that corresponds to an unnamed address, it inserts that name into the name table.

At the end of the search, a message shows the number of unnamed addresses that were in the working name table and how many of those addresses were resolved by searching the selected name file.

To resolve unnamed stations by searching an external file:

1. Compile a list of the addresses. Press F10 **[New capture]** to capture some frames, either live from the network or from a file. Press F10 **[Stop capture]** to stop the capture.
2. Move to **Display\Manage names\Resolve names** and press ENTER.
3. Press F6 **[Display options]**. Move to **Manage names\Look for names** and press ENTER.

   In response, the analyzer displays a list of name files. Move to the file you want to use and press ENTER.
4. To preserve the names you have added, move to **Manage names \Save names** and press Spacebar or ENTER to enable (√) the option. When you exit, the analyzer will copy the names from the working name table to the startup file. It discards addresses without names.

Looking for Names in Captured Frames

Certain protocols, including Novell NetBIOS and TCP DNS, automatically assign names to higher-level addresses and let stations exchange the resulting tables. When the **Look for names** option is enabled (the default), the analyzer automatically scans for such tables during capture and adds the following information to its working name table:

- Names for unnamed addresses that are already in the name table
- Both names and addresses for addresses not yet in the table

It does not, however, revise names for addresses that are already in the table. When it completes the search, the analyzer reports the number of address and name pairs it added to the working name table. By using this option, you may also find higher-level addresses that did not send or receive frames during a particular period of capture.

If the **Look for names** option is enabled, the analyzer automatically updates its working name table with various higher-level addresses and associated names.

To look for names within the frames in the capture buffer:

If the option is disabled, you can:

1. Press F10 **[New capture]** to capture some frames, either live from the network or from a file. Press F10 **[Stop capture]** to stop the capture.
2. Press F3 **[Data display]**.
3. Press F6 **[Display options]** and move to **Manage names \ Look for names** and press ENTER.

   In response, the Sniffer analyzer scans the capture buffer for protocols that exchange name information and adds any new addresses and corresponding names to the working name table.

IMPORTANT: Names found with the **Look for names** option may be transitory. For example, you may find a name that a user assigned for a single work session. The user may then move to another machine and assign the name to a different address. Because machine names are easy to change, you may not want to save a name table constructed this way; the table may be wrong the next time you use it.

Saving the Name Table

When the **Save names** option is enabled, the Sniffer analyzer automatically updates the startup file with the current working name table when you exit, thereby saving any new addresses and names, as well as any changes. If the option is disabled (the default), you must save manually. If you try to exit without saving the names that the

Sniffer analyzer found and added, a warning message appears that allows you to cancel the Exit command.

Addresses that are not named are purged when you exit the Sniffer analyzer regardless of whether the **Save names** option is enabled. Therefore, if you want to save new addresses, be sure to assign them a name.

To automatically save the current working name table:

1. Move to **Display\Manage names\Save names** and press Spacebar to enable (√) the option.

To manually save the current working name table:

1. Move to **Display\Manage names\Save names** and press ENTER.

   In response, the Sniffer copies all named addresses from the working name table to the file c:*xx*SNIFF\STARTUP.*xx*D.

Clearing the Name Table

When the startup file contains names that are no longer appropriate, you can either edit them individually or clear all names and start over.

The **Clear all names** option removes both names and addresses from the working name table. Use this option when you want to start over, perhaps before resolving names from a name file or before looking for embedded names within higher-level protocols in the capture buffer.

IMPORTANT: Using the **Clear all names** followed by the **Save names** option empties the working name table and the name table in the startup file. Use these features carefully.

Saving Captured Frames as Data (Trace) Files

You can save the frames in the capture buffer to a file on the analyzer's hard disk. When saving files, you have the following options:

- Saving everything in the capture buffer
- Saving only those frames that pass the current display filters
- Saving only those frames within a particular range
- Saving any frames you select individually

To save frames in the capture buffer to a file:

1. Press F5 **[Menus]** to return to the main menu. Move to **Files \ Save \ Data** (shown in Figure 8–6).

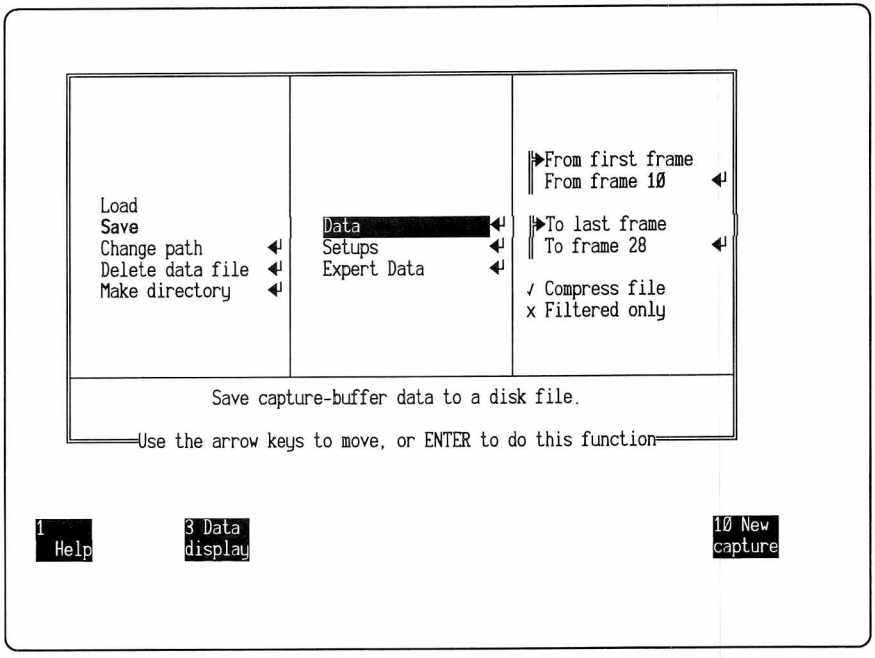


Figure 8–6. Menu to save captured frames to a file

2. (Optional) Set the range of frames to be saved. If you do not want to use the defaults (from first to last), move to the specific numbers and press ENTER. In the dialog box that appears, enter the desired range.

   From first frame
   From frame xx
   From last frame
   To frame xx

3. (Optional) To save only those frames you specifically select, display the Summary view, move to each frame you want to select, and press F9 **[Select frame]**. Then enable the **Selected frames** display filter and redisplay. Continue with step 5.
4. (Optional) To save only those frames that pass the display filters, move to **Filtered only** and press Spacebar to enable (√) the option.
5. To determine whether the file will be saved compressed or uncompressed, move to **Compress file**. Press Spacebar to enable (√) or disable (x) the option.
6. Move to **Data** and press ENTER.

In the dialog box that appears, enter the desired file name (up to eight characters) and press ENTER. Do not include an extension; the Sniffer analyzer automatically attaches the extension .*xx*C, where *xx* stands for the network, such as EN for Ethernet or TR for token ring. If a file with that name already exists, you can abort the request or overwrite the existing file.

The path shows the current drive with the current path (\CAPTURE unless you changed the path). You can backspace over any part of the display and enter the name of a different drive or directory.

Converting Internetwork Analyzer Trace Files to LM2000 Format

The Sniffer Internetwork Analyzer includes a conversion utility that allows you to convert trace files between Sniffer Internetwork Analyzer format and LM2000 Analyzer format. In this way, you can capture a trace file with one application and still use the analysis features offered by the other application.

Using the Sniffer—LM2000 Conversion Utility

Load the Sniffer—LM2000 Conversion Utility from the Main Selection Menu of the Sniffer Network Analyzer. Figure 8–7 shows a sample Main Selection Menu with the Sniffer—LM2000 Conversion Utility highlighted.

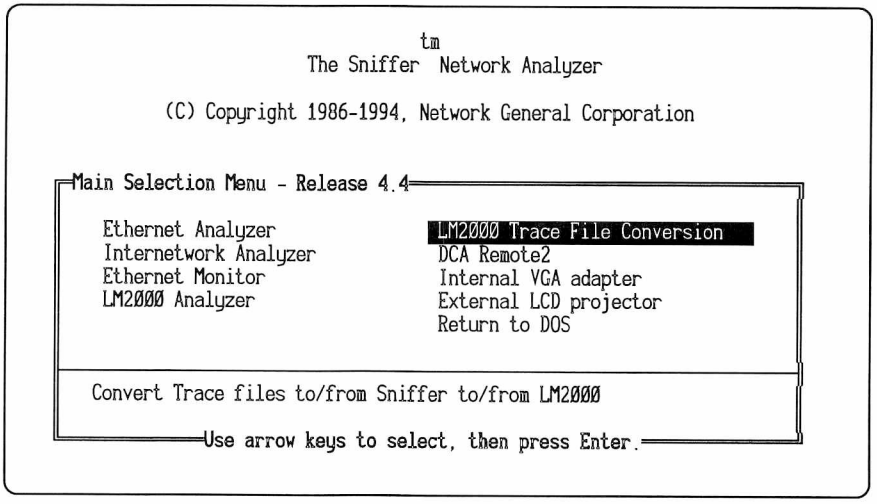


Figure 8–7. Main Menu of the Sniffer Network Analyzer

To convert a trace file between Sniffer Internetwork Analyzer and LM2000 formats:

1. From the Main Selection Menu of the Sniffer Network Analyzer, use the cursor keys to highlight the **LM2000 Trace File Conversion** entry, as in Figure 8–7. Press ENTER.

   The main menu of the LM2000—Sniffer Conversion Utility appears (Figure 8–8).

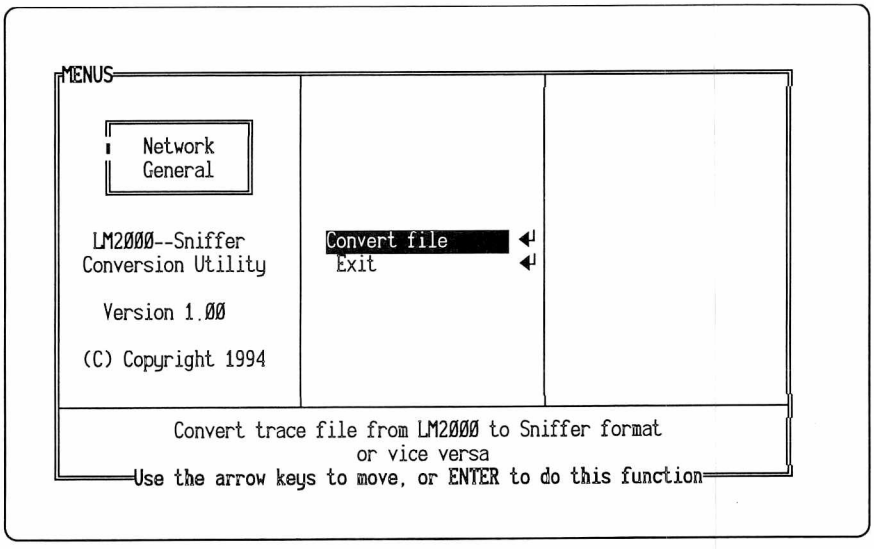

MENUS
Network General
LM2000--Sniffer Conversion Utility
Version 1.00
(C) Copyright 1994
Convert file
Exit
Convert trace file from LM2000 to Sniffer format or vice versa
Use the arrow keys to move, or ENTER to do this function

Figure 8–8. Main menu of the LM2000—Sniffer Conversion Utility

2. By default, the **Convert file** menu entry is highlighted. Press ENTER.

   Result: A window (shown in Figure 8–9) appears listing the files available for conversion in the current directory. You can use the cursor and ENTER keys to move among the various directories.

NOTE: The utility lists only those files the LM2000—Sniffer Conversion Utility can convert. The only files it can convert are those captured by the Sniffer Internetwork Analyzer or the LM2000 Analyzer.

- Files captured by the Sniffer Internetwork Analyzer have the three-letter extension .SYC. For example, a sample trace file could be titled *SAMPLE*.SYC.
- Files captured by the LM2000 Analyzer have the three-letter extension .BUF. For example, a sample trace file could be titled *SAMPLE*.BUF.

Figure 8–9 shows the window that lists convertible files.

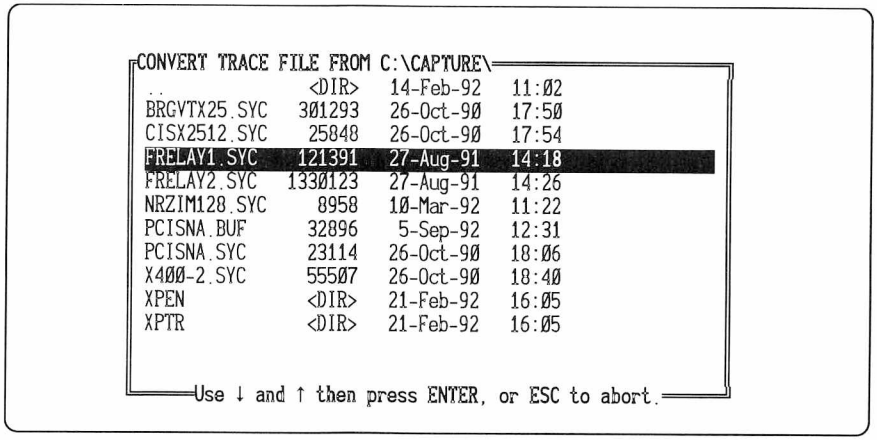

CONVERT TRACE FILE FROM C:\CAPTURE\
.. <DIR> 14-Feb-92 11:02
BRGVTX25.SYC 301293 26-Oct-90 17:50
CISX2512.SYC 25848 26-Oct-90 17:54
FRELAY1.SYC 121391 27-Aug-91 14:18
FRELAY2.SYC 1330123 27-Aug-91 14:26
NRZIM128.SYC 8958 10-Mar-92 11:22
PCISNA.BUF 32896 5-Sep-92 12:31
PCISNA.SYC 23114 26-Oct-90 18:06
X400-2.SYC 55507 26-Oct-90 18:40
XPEN <DIR> 21-Feb-92 16:05
XPTR <DIR> 21-Feb-92 16:05
Use ↓ and ↑ then press ENTER, or ESC to abort.

Figure 8–9. Window for specifying trace file to be converted

3. Use the cursor and ENTER keys to highlight the trace file you want to convert.
   - Trace files for the Sniffer analyzer are stored in the C:\CAPTURE directory.
   - Trace files for the LM2000 Analyzer are stored in the C:\LM2000 directory.

   When you have highlighted the trace file you want to convert, press ENTER.

NOTE: Source trace files for conversion may be located in any directory on the C:\ drive. You cannot, however, convert from trace files located on a floppy diskette. To convert a trace file from a floppy diskette, you must first use the COPY command to copy the desired trace file to the Sniffer analyzer's hard disk. For example, to copy the file A:\TRACE.SYC to the C:\CAPTURE directory, enter the following command at the C:\CAPTURE> prompt:

```
C:\CAPTURE> COPY A:\TRACE.SYC
```

4. The conversion utility prompts you to supply the name and DOS path for the converted file it will create. Do not supply an extension — the utility automatically appends the extension appropriate to the type of trace file it is creating. For example, for an LM2000 trace file, the analyzer appends the extension .BUF. For a Sniffer Internetwork Analyzer trace file, the analyzer appends the extension .SYC. (Figure 8–10 shows the dialog box in which you name the file to be created.)

   If the file you name already exists, the conversion utility displays a warning. You can either overwrite the existing file or press ESC if you want to rename the target file.

   Although you cannot convert a trace file from a drive other than the hard drive (C:\), you can specify a target drive other than C:\. For example, you could elect to write the converted file directly to a floppy diskette. Simply backspace over the provided path and type in the desired path.

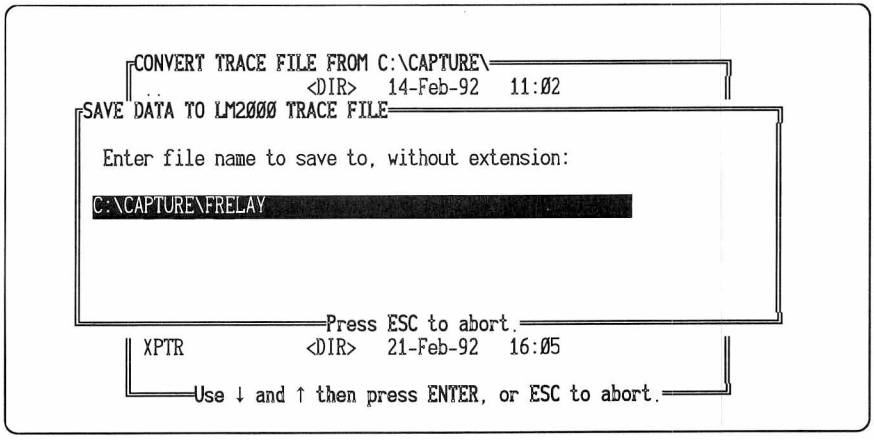

CONVERT TRACE FILE FROM C:\CAPTURE\
.. <DIR> 14-Feb-92 11:Ø2
SAVE DATA TO LM2ØØØ TRACE FILE
Enter file name to save to, without extension:
C:\CAPTURE\FRELAY
Press ESC to abort.
XPTR <DIR> 21-Feb-92 16:Ø5
Use ↓ and ↑ then press ENTER, or ESC to abort.

Figure 8–10. Dialog box for naming converted trace file

5. Once you have named the file to be created, press ENTER. A window will appear indicating the progress of the file conversion. When conversion is complete, the window that lists trace files reappears. From here, you can convert another trace file, or press ESC to return to the main menu of the conversion utility.

A Word About the Dates of Converted Trace Files

When you convert a trace file from LM2000 format to Sniffer analyzer format, the DOS creation date of the new file will be the date to which the computer is currently set[1]. However, when you convert a Sniffer analyzer trace file to LM2000 format, the DOS creation date of the new file will be the timestamp (date of capture) stored inside the Sniffer analyzer trace file. Accordingly, if on September 2, 1993, you converted a Sniffer analyzer trace file with a timestamp of 10-May-91, the created LM2000 file would show a creation date of 10-May-91 rather than 2-Sep-93.

Using Data Files to Load the Capture Buffer

If you save all or part of the capture buffer to a file, you can use the resulting file to load the capture buffer. In this way, you can examine frames captured at another time or place, or frames sent to you for study.

You can load the capture buffer directly from a previously saved file, without starting a capture.

1. You can use the DOS command DATE to change the computer's current date.

To load the capture buffer with a file of saved frames:

1. Move to **Files \ Load \ Data** and press ENTER.

   A dialog box appears that contains an alphabetical list of previously saved capture files and directories. Each filename includes a three-letter extension. The first two letters of this extension identify the network topology. In Figure 8–11, for example, the extension is TRC, which shows that the files were captured from a token ring network. This list includes only those filenames with the proper extensions for the current analyzer.

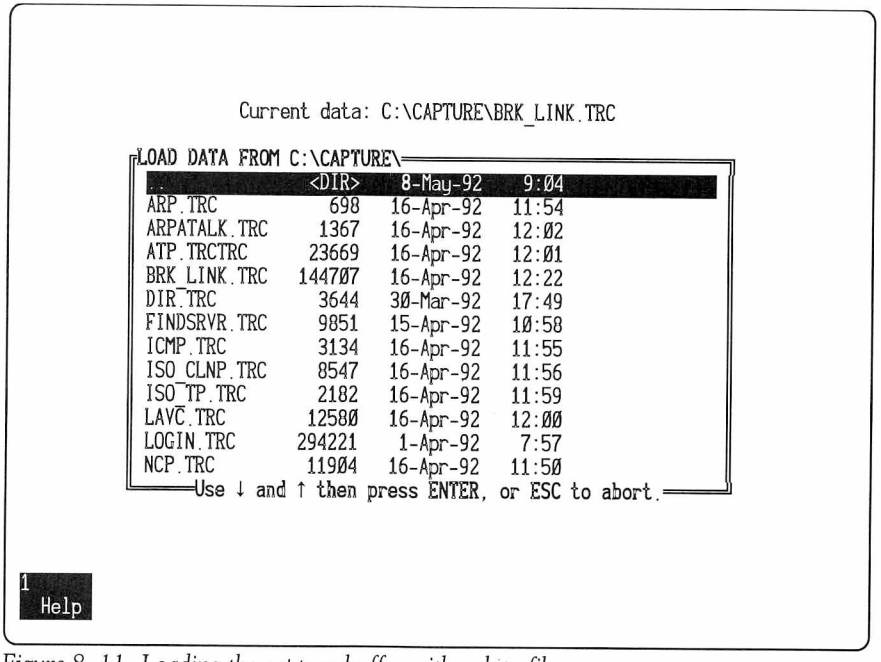

Current data: C:\CAPTURE\BRK_LINK.TRC
LOAD DATA FROM C:\CAPTURE\
.. <DIR> 8-May-92 9:04
ARP.TRC 698 16-Apr-92 11:54
ARPATALK.TRC 1367 16-Apr-92 12:02
ATP.TRCTRC 23669 16-Apr-92 12:01
BRK_LINK.TRC 144707 16-Apr-92 12:22
DIR.TRC 3644 30-Mar-92 17:49
FINDSRVR.TRC 9851 15-Apr-92 10:58
ICMP.TRC 3134 16-Apr-92 11:55
ISO_CLNP.TRC 8547 16-Apr-92 11:56
ISO_TP.TRC 2182 16-Apr-92 11:59
LAVC.TRC 12580 16-Apr-92 12:00
LOGIN.TRC 294221 1-Apr-92 7:57
NCP.TRC 11904 16-Apr-92 11:50
Use ↓ and ↑ then press ENTER, or ESC to abort.
1 Help

Figure 8–11. Loading the capture buffer with a data file

2. To change to a different directory, move to the top of the list, to one of the rows labeled **<DIR>**. This label lets you select the directory one step nearer the root directory. Other entries with the **<DIR>** label are subdirectories. To see the list of files in a subdirectory, move to the subdirectory name and press ENTER.
3. Move to the desired file. (To jump directly to the entries that start with a given letter, type that letter and then move to the desired file.)
4. Press ENTER to load the file.
5. Press F3 **[Data display]** to display the analyzed frames from that file, in the display views you defined.

Deleting Data Files

You can delete data files that contain saved frames for the network for which your Sniffer analyzer is configured.

To delete a data file:

1. Move to **Files\Delete data file** and press ENTER.
2. In the dialog box that appears, move to the file you want to delete and press ENTER. (To move to the desired file quickly, type the first letter of that file. The display jumps to that section of the list.)

   In response, the analyzer displays a Warning dialog box that allows you to cancel the deletion.
3. Press ESC to cancel the deletion or press ENTER to complete it.
4. To delete files in other subdirectories, move to **<DIR>** in the top row. Press ENTER to see the files. You can then delete files in that subdirectory.

Saving Expert Data

When capturing in Expert mode, the analyzer creates a database of Expert information pertaining to the current capture session. You can save some or all of this Expert data to a file in CSV (comma separated values) format. This format enables the data to be imported into spreadsheets and other application programs for further processing. For a complete discussion of the internal structure of these CSV files, see the separate manual dealing with Expert analyzer output file format.

The categories of Expert data you can save are:

- The current settings of the Expert thresholds
- The information from the Global Statistics screen
- The information from the Expert Overview screen
- The network objects found during the current capture session
- The diagnoses that occurred during the current capture session

You can save this data by means of the Scheduled Events feature. You can also save Expert data manually at any time. Press F9 to pause the capture, then press F5 to display the menus. Move to **Files\Save\Expert data**. The following screen will appear:

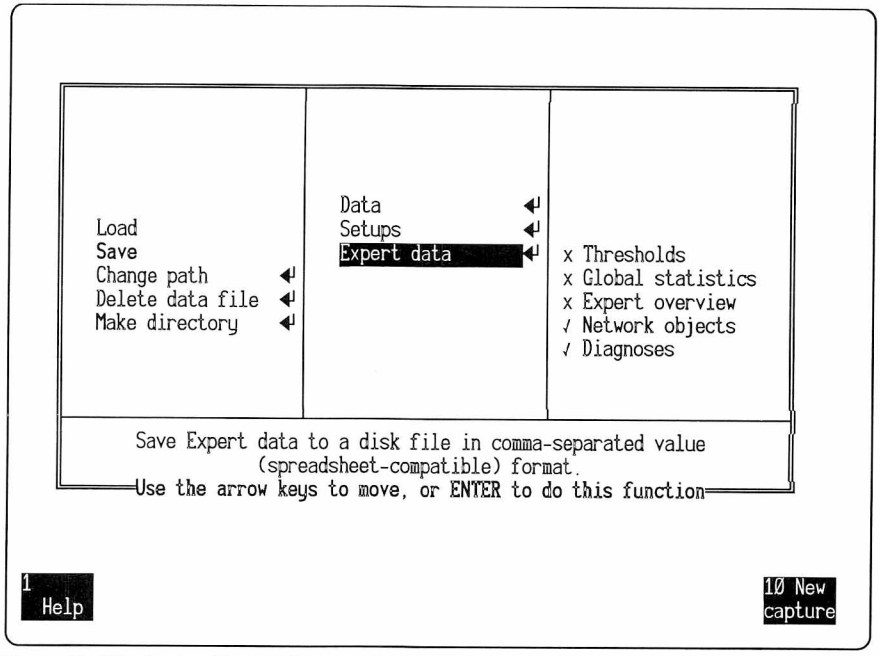


Figure 8–12. Saving Expert data

In the list at the right you can enable or disable each item according to which categories of Expert data you want to include in the file.

In the case of **Network objects**, you can choose the kinds of objects you want to include, as shown in Figure 8–13.

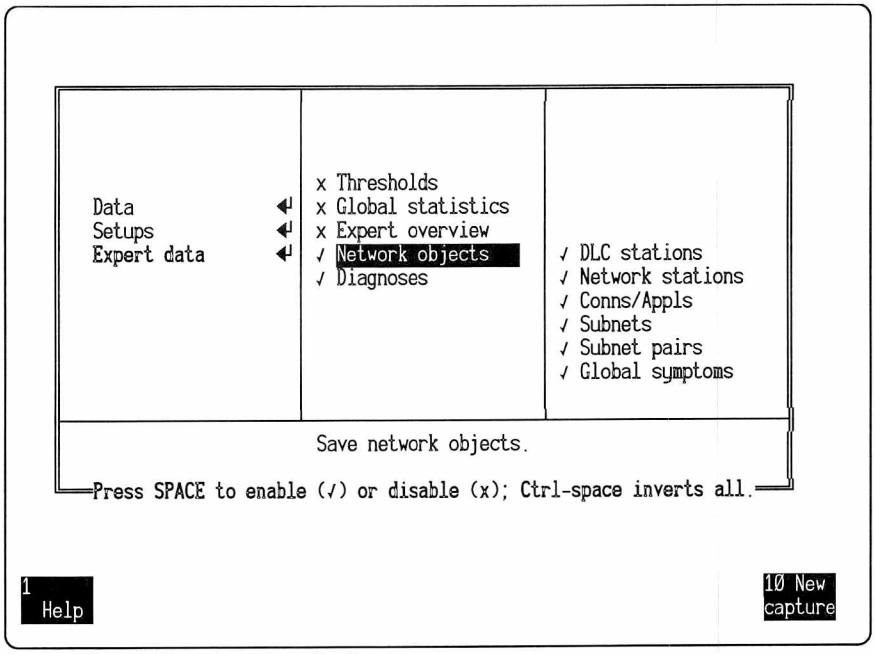


Figure 8–13. Choosing network objects

Similarly, you can choose the layers for **Diagnoses**, as shown in Figure 8–14.

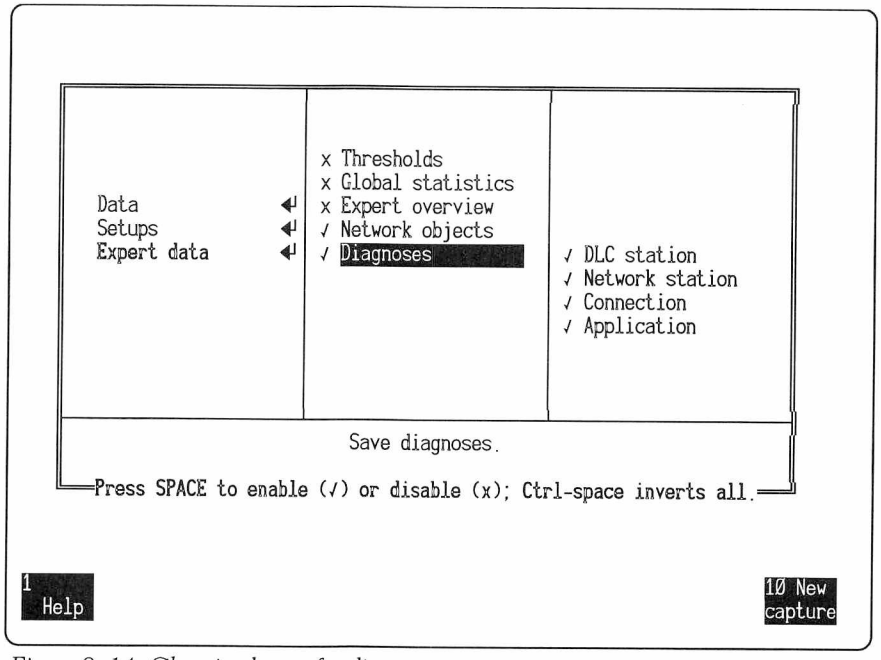


Figure 8–14. Choosing layers for diagnoses

Using Setup Files to Define System Options

In addition to saving files that contain captured data, you can save the "setup" that includes the particular combination of display options, filters, and controls you defined.

If you want to automatically start your analyzer with a particular combination of options, you can save those options to the STARTUP.*xx*S file in the *xx*SNIFF directory. You can also save options to any number of setup files and then load those files to apply particular settings to a capture session.

Contents of a Setup File

The setup file records every option you enabled or disabled, the choices associated with vertical lines (radio control), and all values associated with various options, such as thresholds, file sizes, and so on.

The following options are included in the setup file:

- General system options, such as the **Interpret RI** option
- Capture options, including the capture mode, screen format, and so on.

- Capture filters, including any pattern matches you defined
- Trigger options, including the options associated with the **Disk snapshot** feature
- Display options, including views to be displayed and any associated options
- Display filters, including any pattern matches you defined
- Printer options, such as range of pages to be printed and the file format
- Protocol forcing rules

The following options are not included in a setup file:

- Subnet names, trustee names, or language setting.
- The path you may have set for locating the directory of files to be loaded or saved. However, you can record this path with the DOS SET PATH command.
- The capture buffer. You can save the contents of the capture buffer as a data file (**Files\Save\Data**).
- The name table. You can save the current working name table with the **Display\Manage names\Save names** option.

NOTE: Your setup may refer to addresses (for example, in a station address filter). When you display the filter, you may see the station's symbolic name rather than its numeric address. However, the saved filter does contain the numeric address. The symbolic name will be generated during display, when the analyzer checks the name table for names that correspond to addresses.

Saving the Current Options in the STARTUP File

If the options you need are different from the Network General default options, and if you want your options to be in effect automatically, you can save the options you define to the STARTUP file. As a result, whenever you start the analyzer, it automatically applies the options in that file.

To save your current setup to the STARTUP file:

1. Check your setup to make sure it defines all options as you want them, especially the filters.
2. Move to **Files\Save\Setups** and press ENTER.
3. In the dialog box that appears, type STARTUP. Don't include an extension; the Sniffer analyzer automatically attaches the extension .*xx*S, and stores the file in the *xx*SNIFF directory.

Saving the Current Options as a Setup File

If you want to save a combination of options, but not have them applied automatically at system startup, you can save them to a setup file and then apply them to a particular capture session.

To save your current setup as a setup file:

1. Check your setup to make sure it defines all options as you want them.
2. Move to **Files\Save\Setup** and press ENTER.
3. In the dialog box that appears, type a file name, using no more than eight characters. Don't include an extension; the analyzer automatically attaches the extension *.xx*S, and stores the file in the *xx*SNIFF directory. If that file name is already in use, you can abort the request or overwrite the existing file.

NOTE: You can delete setup files from the DOS command line, if you like.

Applying a Setup File

When you first start the analyzer, it uses the settings in the STARTUP.*xx*S file. If you want to override these settings with a setup file you created, you can do so.

To apply a saved setup file:

1. Move to **Files\Load\Setup** and press ENTER.
2. In the dialog box that appears, move to the desired setup file and press ENTER. In response, the Sniffer analyzer loads the setup file and resets all options as specified in the setup file.

Restoring the Network General Default Options

You may want to restore the default options with which your analyzer was shipped. This is particularly useful if you are getting unexpected results and you want to start from a known state. The default options are illustrated in the *Expert Analysis Application Quick Reference Card.*

To restore Network General's default options:

1. Move to **Options\Use defaults** and press ENTER.

NOTE: This command clears any settings you may have defined. If you think you might want to use these settings again later, save them as a setup file.

Using Protocol Forcing

9

Using Protocol Forcing

Overview

Protocol forcing is an advanced function that allows you to alter the standard interpretive flow through the stacked data found within a predefined set of frames. The set of frames to which the forcing action is applied and the new direction the interpretation will take are defined by up to four rules you can specify prior to displaying the captured data.

This chapter describes how to use the protocol forcing feature. Topics include:

- Specifying a protocol forcing rule
- Applying a protocol forcing rule
- Undoing protocol forcing

Protocol forcing is an advanced tool for network managers to interpret non-standard (for example, proprietary) protocol stacks. For protocol forcing to yield meaningful results, a thorough knowledge of the targeted protocol stack, as well as the way it deviates from the standard, is essential.

How Protocol Forcing Works

Under normal data display, the analyzer displays your captured data based on the parameters you set up in the Display menu options. If you have a non-standard protocol stack that deviates from a given standard, you can use protocol forcing to set up protocol decoding rules that apply to your networking environment. Once these rules are set up, you can apply them to subsequent data displays and file loading.

Protocol forcing affects the data display rather than the data in the capture buffer. The type of protocols available depends on the type of analyzer you have. Protocol forcing is available with the following topologies:

- Ethernet
- Token ring
- FDDI
- Sniffer Internetwork Analyzer (WAN/Synchronous)

Specifying a Protocol Forcing Rule

To specify a protocol forcing rule:

1. In the **Display** menu, enable protocol forcing. Move the highlight to **Protocol forcing** and press Spacebar to toggle between disabled (x) and enabled (✓). Figure 9–1 displays the menu options for Protocol forcing.

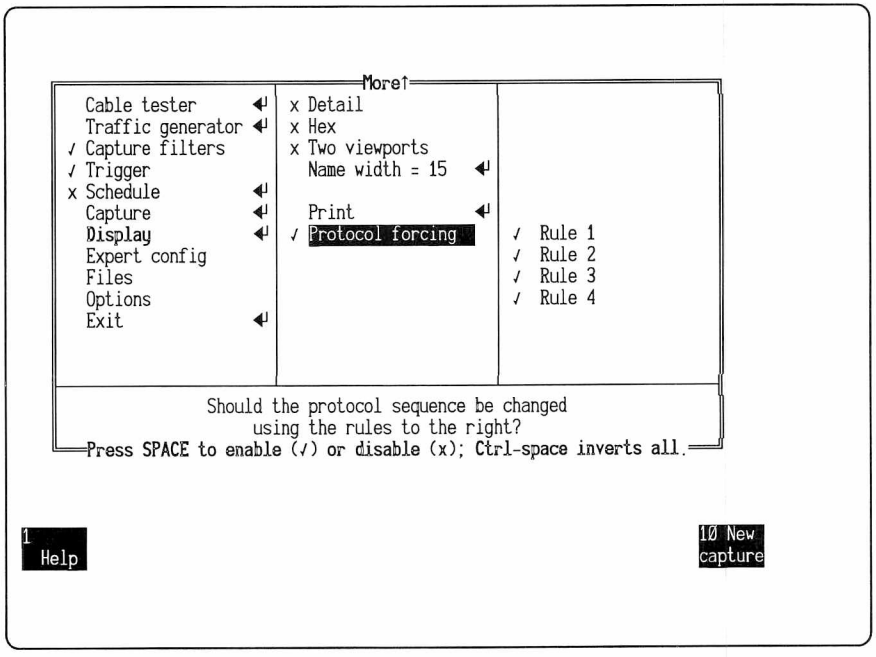


Figure 9–1. Protocol forcing menu options

2. Move to the panel on the right. **Rule 1** will be highlighted. Figure 9–2 displays the options available for **Rule 1**.

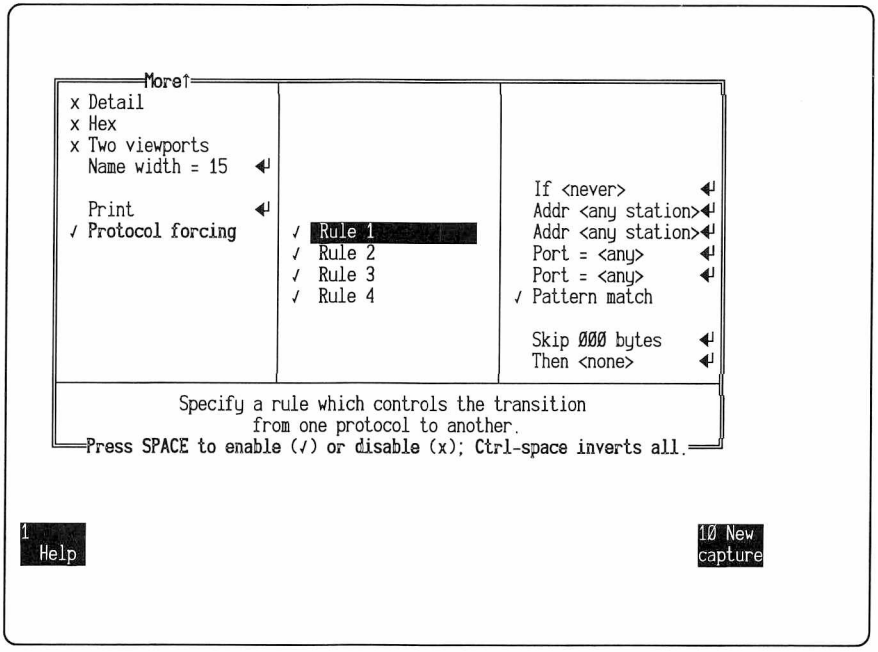


Figure 9–2. Protocol forcing rule options

3. Specify the rule you want the analyzer to use.

   a. In the panel to the right, select the protocol you want to force.

      Highlight the **If** option and press ENTER. The analyzer displays the list of protocols available through the set of protocol interpreter suites installed. This selection is considered the "force from" protocol (Figure 9–3). Scroll through the list to highlight the protocol you want to force and press ENTER.

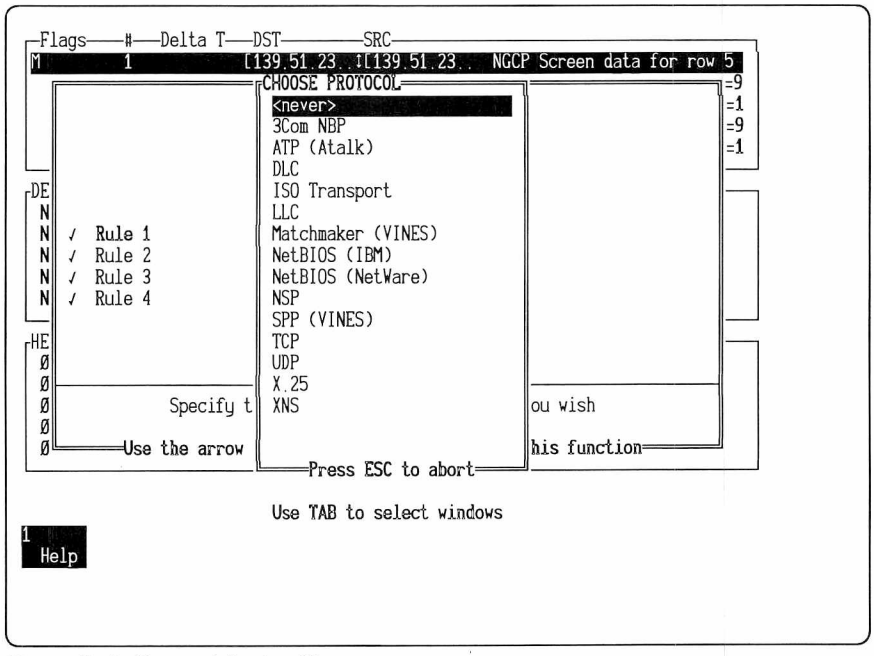


Figure 9–3. Protocol forcing If menu

b. Press ENTER at the **Addr** option(s) to specify a frame address to restrict the use of the rule.

   A name table is displayed (Figure 9–4). The name table is the same for both the source and destination stations. If you have already displayed your data, the name table highlights the source or destination frame from the display. You can restrict the use of the rule to both the source and destination stations.

   Scroll through the name table to highlight the station you want and press ENTER. Select the second **Addr** option if you want to select the destination station.

NOTE: This field name is based on the **If** protocol selected.

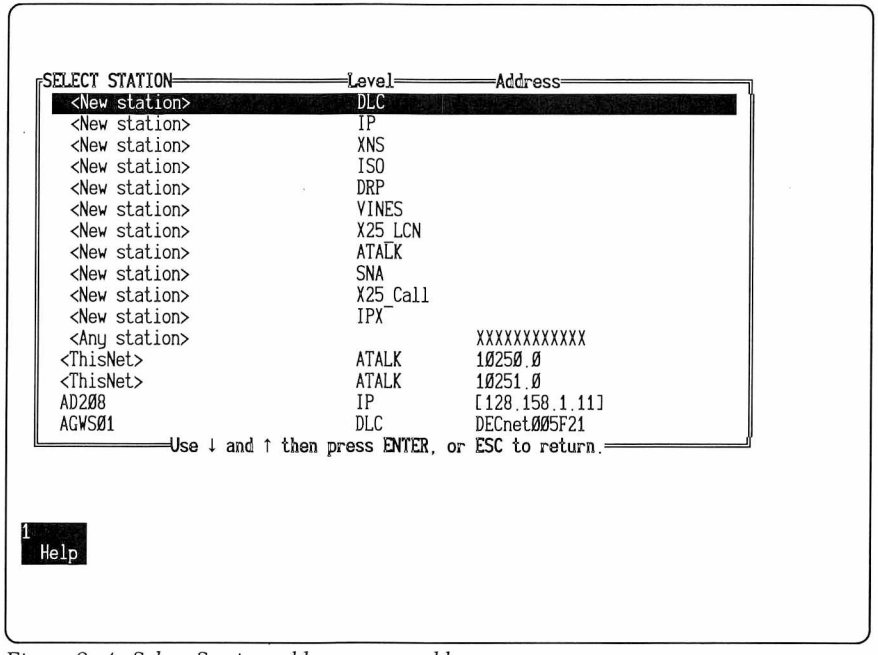


Figure 9–4. Select Station address name table

c. Press ENTER at the **Port** option(s) to specify a protocol port to restrict the use of the rule.

A pop-up window displays the current valid port type (Figure 9–5). This is the connection identifier for the two stations. The analyzer provides the current socket number of the frame. You can select **Specify a value** to specify your own value. The protocol port type varies depending on the **If** protocol selected.

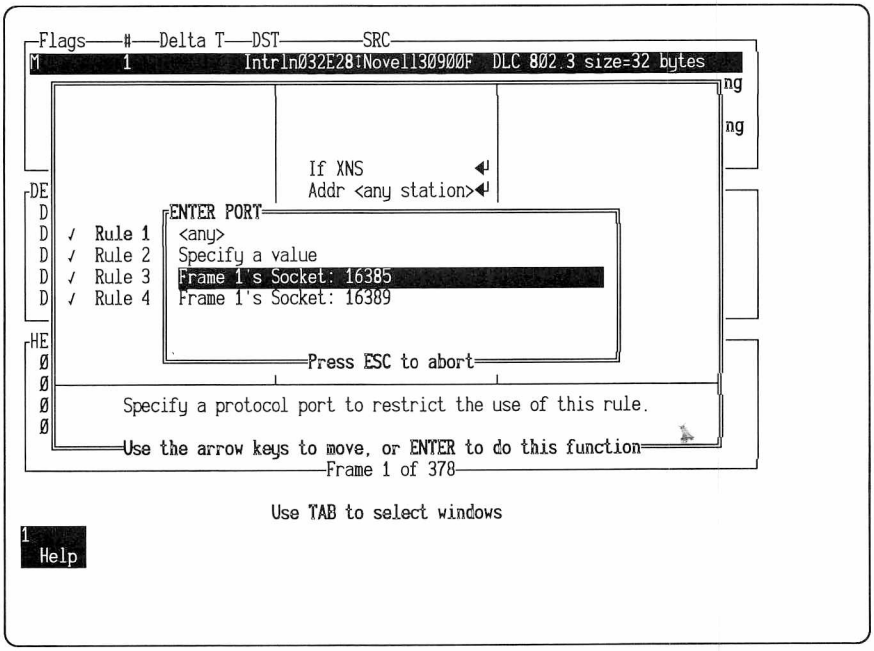


Figure 9–5. Port option window

d. Specify a pattern that must be present in a frame for the rule to be used.

   Refer to the section "Pattern Match Filter" on page 6–45 of this manual for information on using the pattern match options.

e. Specify the byte offset in hex from the end of the **If** protocol header to the start of the **Then** protocol header.

   Figure 9–6 displays the pop-up window where you can specify a hex offset.

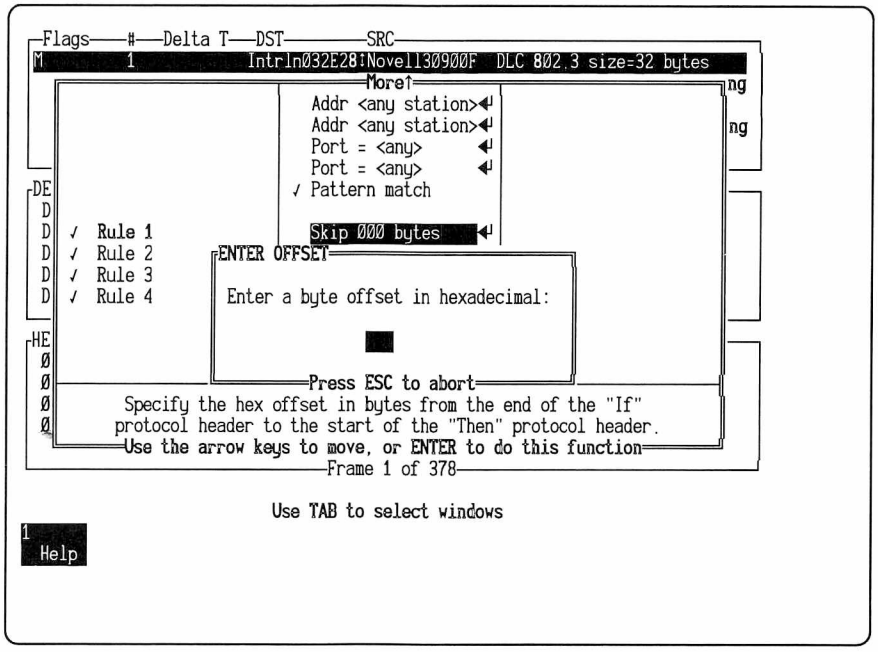


Figure 9–6. Byte offset window

f. Press ENTER at the **Then** option to specify the protocol that should be used as the "force to" protocol.

   A list of available protocol options is displayed. This selection is considered the "force to" protocol (Figure 9–7). Scroll through the list to highlight the protocol that should be used as the "force to" protocol and press ENTER.

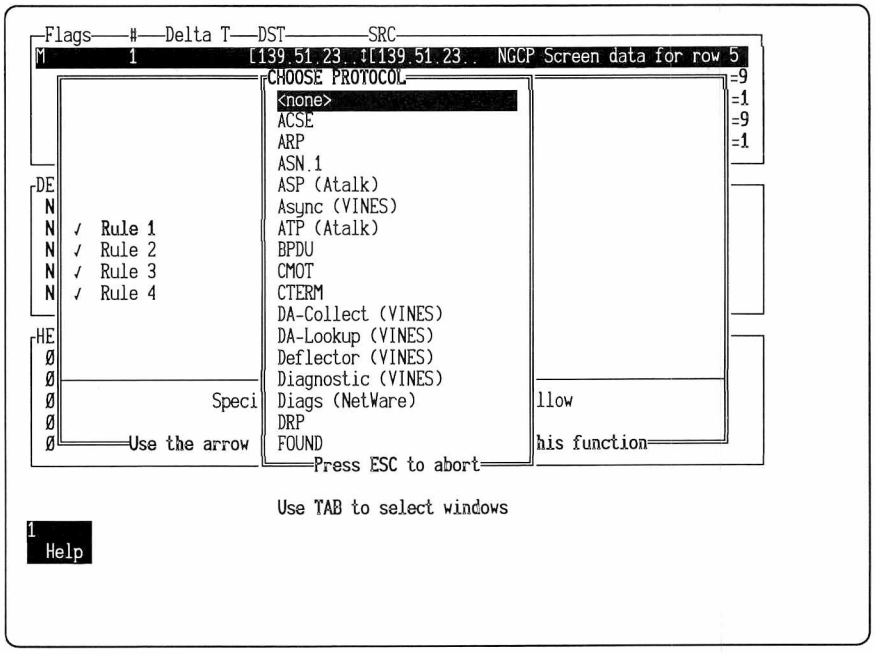


Figure 9–7. Protocol forcing Then menu

4. To specify additional rules (Rule 2 to Rule 4), repeat step 3.

Applying a Protocol Forcing Rule

Under normal data display, the analyzer displays your captured data as shown in Figure 9–8. The procedure below uses protocol forcing to change the display.

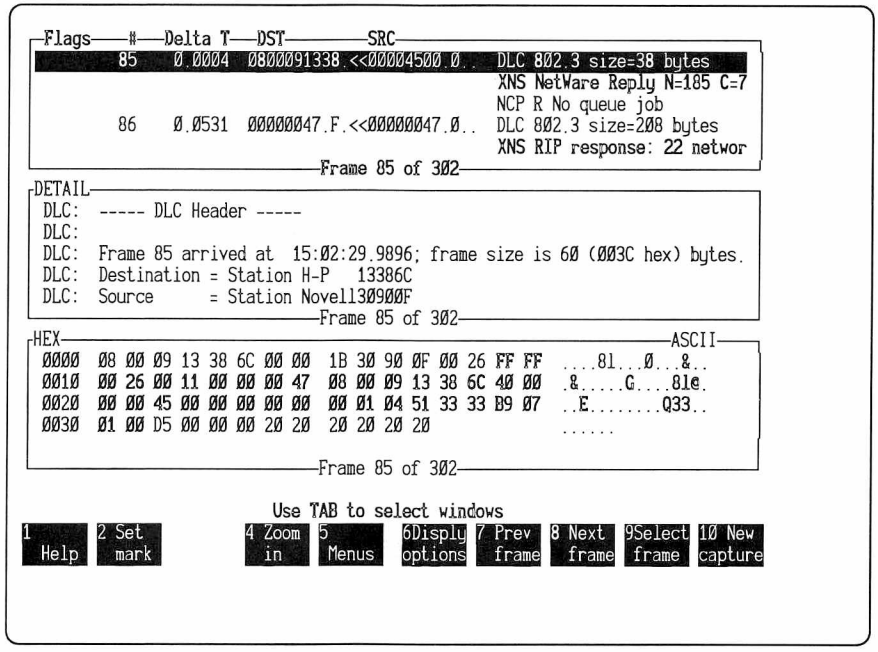

Flags—#—Delta T—DST—SRC
85 0.0004 0800091338.<<00004500.0.. DLC 802.3 size=38 bytes
XNS NetWare Reply N=185 C=7
NCP R No queue job
86 0.0531 00000047.F.<<00000047.0.. DLC 802.3 size=208 bytes
XNS RIP response: 22 networ
Frame 85 of 302
DETAIL
DLC: ----- DLC Header -----
DLC:
DLC: Frame 85 arrived at 15:02:29.9896; frame size is 60 (003C hex) bytes.
DLC: Destination = Station H-P 13386C
DLC: Source = Station Novell30900F
Frame 85 of 302
HEX
ASCII
0000 08 00 09 13 38 6C 00 00 1B 30 90 0F 00 26 FF FF ....8l...0...&..
0010 00 26 00 11 00 00 00 47 08 00 09 13 38 6C 40 00 .&.....G....8l@.
0020 00 00 45 00 00 00 00 00 00 01 04 51 33 33 B9 07 ..E.....Q33..
0030 01 00 D5 00 00 00 20 20 20 20 20 20 ......
Frame 85 of 302
Use TAB to select windows
1 Help
2 Set mark
4 Zoom in
5 Menus
6Disply options
7 Prev frame
8 Next frame
9Select frame
10 New capture

Figure 9–8. Display without protocol forcing

To apply a protocol forcing rule:

1. Enable protocol forcing from the **Display** menu: Move the highlight to **Protocol forcing** and press Spacebar to toggle between disabled (x) and enabled (✓).
2. Select the rule you want to use. Move the highlight to that rule and press Spacebar to toggle between disabled (x) and enabled (✓). Refer to "Specifying a Protocol Forcing Rule" on page 9–4 for information on setting a protocol forcing rule. Figure 9–9 displays the rule used in this procedure.

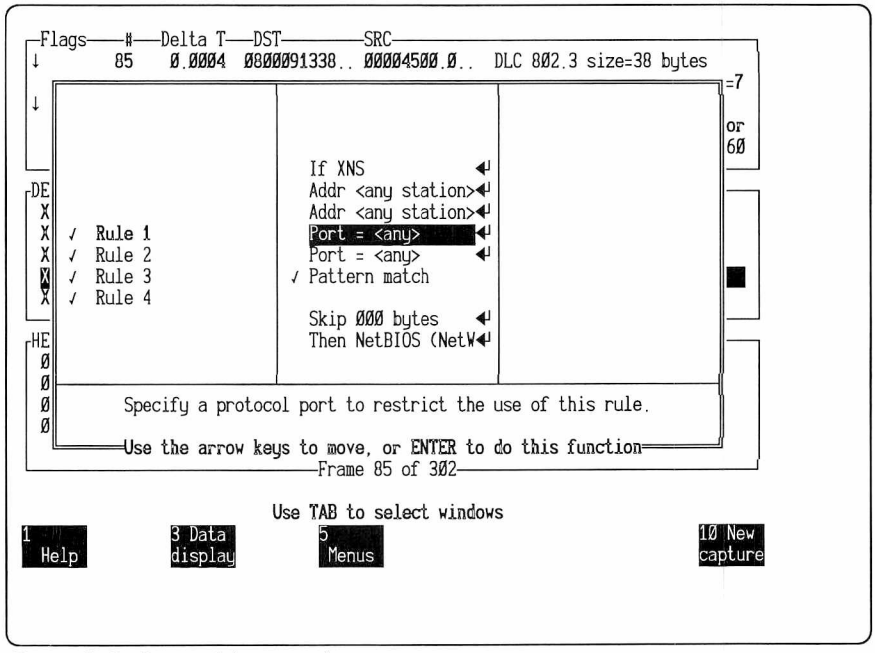


Figure 9–9. Protocol forcing rule

3. Select **Flags** in the Summary menu.

   Activating Flags allows you to see quickly which frames in the Display/Summary view are affected by protocol forcing. For additional information on the flags options, refer to the section "Flags Display Option" on page 7–40.

4. Press F3 to display frames in the capture buffer. To make use of **Protocol forcing**, it is generally useful to enable **Summary, Detail**, and **Hex** views.

   The **Summary** view displays a down arrow before each frame with a forced protocol. Also, the color display changes from its normal display to indicate a forced protocol.

   The **Detail** view displays a "Forced to <protocol>" in the protocol field corresponding to the **Then** option of your rule.

   Figure 9–10 shows the data display with protocol forcing applied to it.

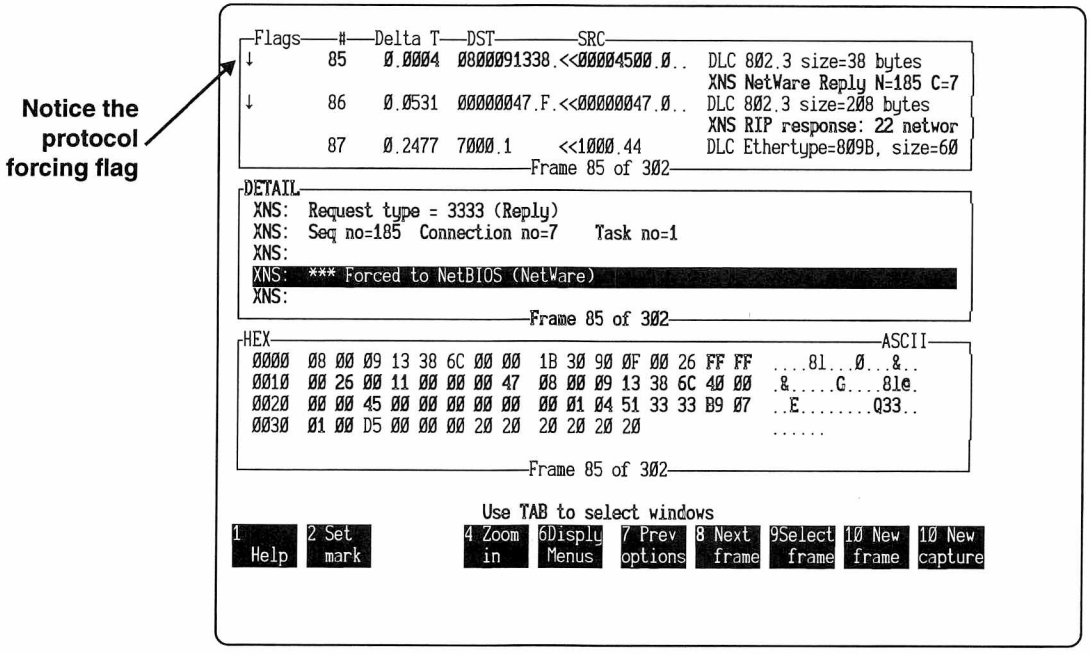

Notice the protocol forcing flag
Flags
#
Delta T
DST
SRC
↓ 85 Ø.ØØØ4 ØØØØØ91338.<<ØØØØ4500.Ø.. DLC ØØ2.3 size=38 bytes
XNS NetWare Reply N=185 C=7
↓ 86 Ø.Ø531 ØØØØØØ47.F.<<ØØØØØØ47.Ø.. DLC ØØ2.3 size=2Ø8 bytes
XNS RIP response: 22 networ
87 Ø.2477 7ØØØ.1 <<1ØØØ.44 DLC Ethertype=ØØ9B, size=6Ø
Frame 85 of 3Ø2
DETAIL
XNS: Request type = 3333 (Reply)
XNS: Seq no=185 Connection no=7 Task no=1
XNS:
XNS: *** Forced to NetBIOS (NetWare)
XNS:
Frame 85 of 3Ø2
HEX
ASCII
ØØØØ Ø8 ØØ Ø9 13 38 6C ØØ ØØ 1B 3Ø 9Ø ØF ØØ 26 FF FF ....8l...Ø...&..
ØØ1Ø ØØ 26 ØØ 11 ØØ ØØ ØØ 47 Ø8 ØØ Ø9 13 38 6C 4Ø ØØ .&.....G....8l@.
ØØ2Ø ØØ ØØ 45 ØØ ØØ ØØ ØØ ØØ ØØ Ø1 Ø4 51 33 33 B9 Ø7 ..E.........Q33..
ØØ3Ø Ø1 ØØ D5 ØØ ØØ ØØ 2Ø 2Ø 2Ø 2Ø 2Ø 2Ø ......
Frame 85 of 3Ø2
Use TAB to select windows
1 Help
2 Set mark
4 Zoom in
6Disply Menus
7 Prev options
8 Next frame
9Select frame
1Ø New frame
1Ø New capture

Figure 9–10. Display using protocol forcing

Disabling Protocol Forcing

Protocol forcing has a temporary effect on the display. If you close the display, or replace the contents of the capture buffer, the analyzer discards any protocol forcing you did earlier. When you save the capture buffer, the saved file does not contain any record of the protocol forcing you may have applied to it.

While a display is active, the **Display options** menu gives you a way to undo the forcing of individual frames.

To undo a forced protocol:

1. From the **Display options** menu, highlight **Protocol forcing**.
2. Disable protocol forcing entirely or disable one or more individual rules: Move the highlight to either **Protocol forcing** or a rule you want to disable and press Spacebar to toggle from √ (enabled) to x (disabled).

   The analyzer returns the display to its previous form.

Special Considerations for Protocol Forcing

There are some special considerations that apply to the protocol forcing process:

- You cannot use protocol forcing to interpret a protocol that occurs prior to the end of a DLC header.
- For most networks, the expert system can use the protocol forcing rules only if SNAP is the protocol *from* which you are forcing (that is, if you have selected SNAP from the **If** list).

  However, on a Sniffer Internetwork Analyzer, the expert system can use the protocol forcing rules if you are forcing *from* any of the following protocols:

  DLC
  HDLC
  PPP
  X.25
  Frame Relay
  SNAP
  Embedded Ethernet

  For example, to view SNMP frames embedded in HDLC, you can use the protocol forcing rule: If HDLC then Ethernet.
- When you capture from a trace file, you should enable the protocol forcing rules before you start the capture. In this way you will assure that the interpretation of the frames will benefit from any available information involving interframe dependencies.

  If you find that you have captured from a trace file without enabling the desired protocol forcing rules, you can correct the situation by pressing F6 **[Disply Options]** and selecting **Reinterpret**. You can also use **Reinterpret** after changing your rule selection to avoid having to capture the file again.

Generating Traffic

10

Generating Traffic

Overview

The **Traffic generator** lets you load a portion of the network with background traffic. This allows you to observe how other stations respond to delays introduced by a large volume of unrelated traffic, to test the response of an individual station to heavy traffic of a particular type, or to test gateways and bridges. Traffic generation is available for the following network topologies:

- Ethernet
- Token ring
- ARCNET
- PC Network
- StarLAN
- FDDI

Frames generated by the Traffic generator obey the network's normal rules for transmitting. For a CSMA/CD network such as Ethernet, that means using the standard collision-detection and back-off algorithms. For a token-passing network, it means waiting for a free token and following the appropriate low-level transmission protocol.

You can use the Traffic generator in two ways:

- Sending the same frame repeatedly **(Single frame mode)**
- For Ethernet, token ring, and FDDI networks, sending the contents of the capture buffer **(Buffer mode)**

If you send the capture buffer, you can choose whether to send all frames or only those that pass the display filters. You can also send the buffer only once or continuously.

If you send the same frame repeatedly, you can specify the frame's destination, size, interval between frames, the maximum number of frames sent, and the content of the first 32 data bytes. By specifying the data bytes appropriately, you can generate frames that appear to the recipient to have a particular SAP or Ethertype address. You can also generate frames to which no station should respond.

Traffic Generator Menu Overview

Figure 10–1 provides an overview of the basic menu items associated with the Traffic generator menu, including those items associated with the **Single frame mode**. Note that, although the figure shows the menu as it appears for an Ethernet network, the basic Traffic generator menu items are the same for all networks.

As with all Sniffer menu options, press the Cursor keys to move the highlight to the desired option and then define that option.

- For options marked with the √ and x symbols, you can press Spacebar to enable (√) or disable (x) the option.
- For options connected with a vertical bar, you can choose one of those options by moving to it and pressing Spacebar.
- For options where you must define a specific value, such as the transmission delay, you can either choose that value from a list or enter the desired value into a dialog box.

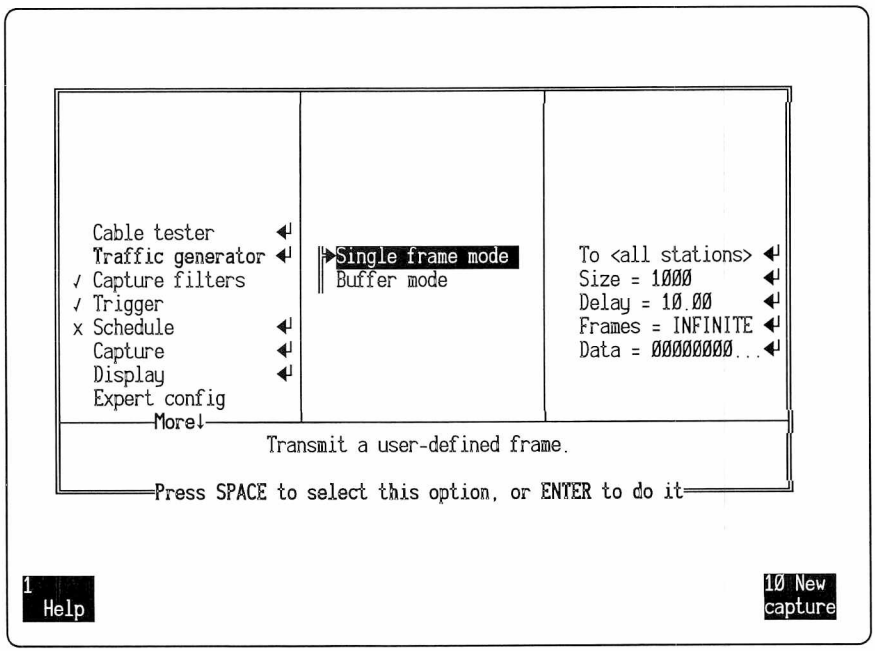


Figure 10–1. Traffic generator menu options

Preparing to Generate Traffic: Single Frame Mode

When you choose the **Single frame mode** option, the analyzer repeatedly sends the same frame to the destination you specify. You can also specify the frame's contents, including:

- Destination address
- Size of the frame
- Delay, which is the interval between frames
- The maximum number of frames sent
- Data, which consists of the 32 data bytes

Specifying Destination

The destination must be a DLC-level address. The default is **To <all stations>**, which is a broadcast address, but you can also choose the address of a specific station. Depending on the network, there may also be various classes of group addresses.

To specify the destination of the generated frames:

1. Move to **Traffic generator\Single frame mode\To ...** and press ENTER.
   In response, the analyzer displays the list of DLC addresses currently in the working name table.
2. Move to the desired destination address and press ENTER. Note that the **To** field now shows the name of that address (such as To "James") or the numeric address if the station is not named (such as "To "IBM 002FEB").
3. To add a new address to the working name table, move to **<New station>** and press ENTER.
4. In the dialog box that appears, enter the new DLC address and a corresponding name. To select the new address as the destination, repeat step 2.

Specifying Frame Size

The **Size** option determines the total length of the frame to be generated. The minimum and maximum permissible size values depend upon the network, as shown in Figure 10–2.

	Ethernet	Token Ring		FDDI
		4 Mbits/s	16 Mbits/s	
Minimum bytes	12	18	18	18
Maximum bytes	1514	4458	17954	4500

Figure 10–2. Size ranges of generated frames

NOTE: The upper limit for the size of a generated frame has changed slightly in Token Ring-II. To see the correct limits, move to analyzer menu selection **Traffic generator/Single frame mode/Size** and press ENTER. A dialog box will appear, and will specify the minimum and maximum frame size (including the source and destination addresses and the data field).

On Ethernet, the length of the smallest valid frame is 60 bytes. Shorter frames normally occur only as collision fragments. However, the Sniffer analyzer can generate short frames. When you specify a length shorter than 60 bytes, the analyzer displays a warning that other stations may see these as collision fragments and therefore report them as network errors.

The analyzer reports the lengths of captured frames in decimal numbers. The length is the total length ignoring the physical header and trailer.

To specify the size of the frames to be generated:

1. Move to **Traffic Generator\Single frame mode\Size=** and press ENTER.
2. In the dialog box that appears, enter the desired length and press ENTER.

Specifying the Delay Between Generated Frames

The **Delay** option determines the interval between the time after the Sniffer finishes sending one frame until it starts to send another. The interval is the *minimum* interval between the transmitted frames. The *actual* interval may be longer, since the analyzer may have to wait its turn if other stations are also transmitting.

To specify the delay between generated frames:

1. Move to **Traffic Generator\Single frame mode\Delay** and press ENTER.
2. In the dialog box that appears, type the desired length of the delay (in milliseconds) and press ENTER.

The minimum and maximum interval values are shown in Figure 10–3.

NOTE: On platforms with 486-66MHz processors, the minimum delay is 0.02 msec.

Delay	Ethernet	Ethernet-II	Token Ring	FDDI
Minimum delay, milliseconds	0.04	0.025	1.0	0.13
Maximum delay, milliseconds	1000	1000	1000	1000

Figure 10–3. Interval ranges between consecutive generated frames

Specifying the Number of Frames to Generate

The **Frames** option determines the number of frames to be sent, from 1 to 999999999. The default is "Infinite," which means the analyzer transmits frames until you press ESC.

To specify the number of frames to be generated:

1. Move to **Traffic Generator\Single frame mode\Frames** and press ENTER.
2. In the dialog box that appears, type the number of frames you want to transmit and press ENTER. To return to the default "Infinite," type 0.

Defining the Frame's Data Field

The generated frame's destination and source fields use the first twelve bytes, as shown in Figure 10–4. The rest of the frame is considered "data," of which you can specify the first 32 bytes. The last four bytes in the data field shows the frame sequence number.

When defining the contents of the data field, you must consider whether the frame will contain routing information. For more information, refer to "Specifying the RI Bit in Generated Frames" on page 10–9.

Structure of a Generated Frame

Figure 10–4 shows the fields in a generated frame.

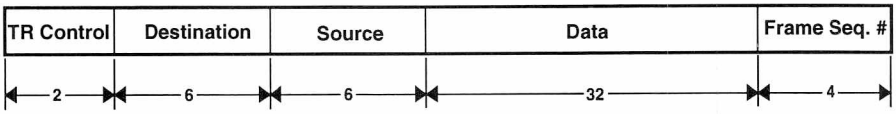


Figure 10–4. Structure of a generated frame

Control	(Token ring and FDDI only) Two bytes that specify media access and/or frame control.
Destination	Six bytes that specify the destination, chosen with the **To <all stations>** option.
Source	Six bytes generated by the Sniffer to identify itself.
Data	Up to 32 bytes available for data. If you do not specify all 32 bytes, the remaining bytes are padded with 00 hex.
Frame Seq. #	The last four bytes, generated automatically by the Sniffer (one for the first transmitted frame of a series, increased by one for each additional frame to correspond with the decimal frame number).

To specify the contents of the data field:

1. Move to **Traffic Generator/Single frame mode/Data =** and press ENTER.
   In response, the Sniffer displays a dialog box that contains 64 zeros (32 repetitions of 00 hex).
2. Type the data you want, in hex, and press ENTER. Any positions you do not specify remain as 0.
   If the total length of the data field is less than 32 bytes, the analyzer takes the number needed and ignores the rest. If the total length of the data field is greater than 32 bytes, the analyzer fills the additional space with 00 hex.
   The Sniffer analyzer also inserts the sequence number for the generated frame into the last four bytes of the data field. Thus, when the total length of the data field is less then 32 bytes, the sequence number overwrites those positions of the data field.

IMPORTANT: If the generated frames are sent to a real station and you expect that station to read them, you must supply reasonable values in the first part of the data

field. For example, an Ethernet recipient will expect to see an Ethertype, an 802.3 recipient will expect to see length information and an 802.2 header, and so on.

Specifying the RI Bit in Generated Frames

A frame that originates on a token ring network may also include an RI field. The RI fields, which contain a record of each intermediate station that forwarded the frame, are located after the usual DLC source and destination fields. (For a more detailed description of the routing field, see "About the Interpret RI Option" on page 3–5.)

Modifying the Source Address for RI Fields

To indicate that these optional fields are present, the source address must be modified by forcing a 1 in the bit that (in a destination address) indicates a "broadcast." You cannot control the source address of a generated frame because that frame automatically uses the source address of the analyzer that sent it. However, you can force the analyzer to insert the "RI present" bit.

If you choose to generate frames with the RI bit enabled, it is your responsibility to include a consistent RI header at the beginning of the data field.

To turn on the RI bit in the source address of a generated frame:

1. Move to **Traffic Generator\Single frame mode\Data\RI present** and press Spacebar to enable the option.

Specifying the Length of the RI Field

When the data you specify includes an RI field, you must specify the number of bytes the RI field occupies. The RI field starts with a 2-byte header, followed by a range from zero to eight 2-byte segment addresses.[1] Thus, the total length of the RI field may range from 2 to 18 bytes. The length (mod 32) is encoded in the low-order five bits of the first byte.

Effect of Routing Information on the Data Field's Layout

When a frame contains an RI field, that field starts in the third byte after the source address. If there is no routing information, the 802.2 header or the Ethernet data starts with the third byte.

You cannot specify what goes into the first 32 bytes until you decide whether the generated frame contains routing information. Moreover, if the frame does contain

1. These are not DLC addresses, but segment identifiers adopted by mutual agreement.

routing information, the RI field can be of variable length. Unless you declare its length correctly, the recipient cannot locate the fields that follow.

Figure 10–5 summarizes the factors that affect the data field for Ethernet and token ring networks.

<table>
<tr><th colspan="2">Ethernet</th><th>Token Ring</th></tr>
<tr><td colspan="2">The hex characters you enter specify the first 32 data bytes; that is, those that follow the 6-byte destination and 6-byte source address.</td><td>The hex characters you enter specify the first 32 data bytes; that is, those that follow the 1-byte access control, the 1-byte frame control, the 6-byte destination and the 6-byte source address.</td></tr>
<tr><td colspan="2">If the RI field is enabled, the variable length source routing information follows the first two bytes of user-definable data.</td><td>If the RI field is enabled, the first byte of the 32 bytes contains the source routing information.</td></tr>
<tr><td colspan="2">The interpretation of the first two data bytes depends on whether you generate Ethertype or IEEE 802.3 frames.</td><td>The first data byte (following the RI field, if enabled) identifies the destination SAP, the second identifies the source SAP. The next one or two bytes are control bytes that indicate the type of transmission.</td></tr>
<tr><td>Ethertype
The first two bytes are the Ethertype. For example, 0800 identifies the IP Ethertype, while 0600 identifies XNS.</td><td>802.3
The first two bytes are the 802.2 length, followed by the variable-length RI field, followed by the 802.2 header.</td><td></td></tr>
</table>

Figure 10–5. Location of the user-definable data in a generated frame

The placement of the RI field within an Ethertype frame and within an IEEE 802.3 frame is summarized in Figure 10–6.

	Based on <To xxxxxx>	Automatic	Controlled by what you specify for the first 32 bytes			
Ethertype	Destination 6 bytes	Source 6 bytes	Etype 2 bytes	RI 0-32 bytes	Rest of data	
802.3	Destination 6 bytes	Source 6 bytes	Length 2 bytes	RI 0-32 bytes	802.2 header 3-4 bytes	Rest of data

Figure 10–6. Position of RI field in Ethertype and IEEE 802.3 frames

Sequence Numbers

The last four bytes of each frame transmitted by the **Traffic generator** contain a sequence number. Each time you start the **Traffic generator**, the sequence numbers start at 1. If the last four bytes overlap the first 32 data bytes, the sequence number overwrites some of the data you specified for the first 32 bytes.

Preparing to Generate Traffic: Buffer Mode

Buffer mode is available for Ethernet, token ring, and FDDI networks. When you choose the **Buffer mode** option, the Sniffer analyzer sends the contents of the capture buffer instead of specified frames. Depending on the network, some frames are not transmitted. On token ring networks, for example, the analyzer transmits no MAC frames. On FDDI networks, the analyzer transmits all frames in the buffer except MAC frames and Void frames.

NOTE: FDDI analyzers and analyzers with Ethernet-II adapter cards can also transmit frames with CRC errors.

You can use the **Buffer mode** option in conjunction with the **Frame editing** option—which allows you to edit the contents of the frames in the capture buffer—to build and send a complex capture buffer. For more information about this option, see "Using Hexadecimal View to Edit Frames" on page 7–53.

In this mode, you can define:

- Whether to send the buffer contents once or continuously
- Whether to send all frames or only those that pass the Display filters.

Figure 10–7 shows the options associated with the **Buffer mode** option when using the **Traffic generator**.

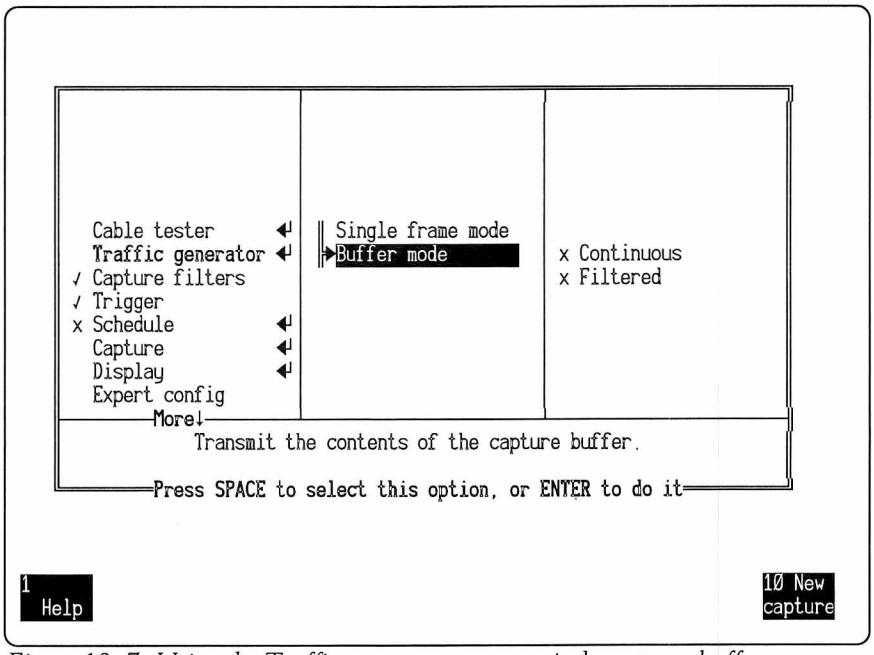


Figure 10–7. Using the Traffic generator to transmit the capture buffer

To generate traffic in buffer mode:

1. Move to **Traffic generator\Buffer mode** and press Spacebar to enable (√) the option.
2. Move to **Continuous** and press Spacebar to enable (√) or disable (x) the option.

   If this option is disabled, the buffer contents are transmitted just once, starting with the first frame through the last frame in the buffer. If the option is enabled, the analyzer transmits its buffer contents repeatedly until you press ESC.
3. Move to **Filtered** and press Spacebar to enable (√) or disable (x) the option.

   If this option is disabled, all frames in the capture buffer are transmitted. If this option is enabled, only those frames that pass the display filters are transmitted. Whether the frames are transmitted continuously or just once depends on the **Continuous** option.
4. FDDI only: Move to **Override SRC Addr** and press Spacebar to enable (√) or disable (x) the option.

   If this option is enabled, the source addresses of all frames in the buffer are replaced with the address of this analyzer. If it is disabled, the analyzer transmits the frames exactly as they are in the buffer.

   Enabling this option assures that the traffic you generate will be stripped off the ring, rather than going around the ring more than once.

However, overriding the source address does not change the source address in the upper-layer fields. Therefore, using the traffic generator to send SMT frames, which also contain a source address, can cause strange behavior on the ring, such as reconfiguring ring maps.

Starting and Stopping Traffic Generation

After you choose the desired **Traffic generator** mode and define the options associated with that mode, you can start to generate traffic.

To start the Traffic generator:

1. Move to **Traffic generator** and press ENTER.

   The Sniffer analyzer starts to transmit frames, as shown in Figure 10–8. This screen updates a counter that shows the current frame number, as well as three thermometer-style bar graphs that show the number of frames transmitted, the number of Kbytes transmitted, and the percentage of network utilization.

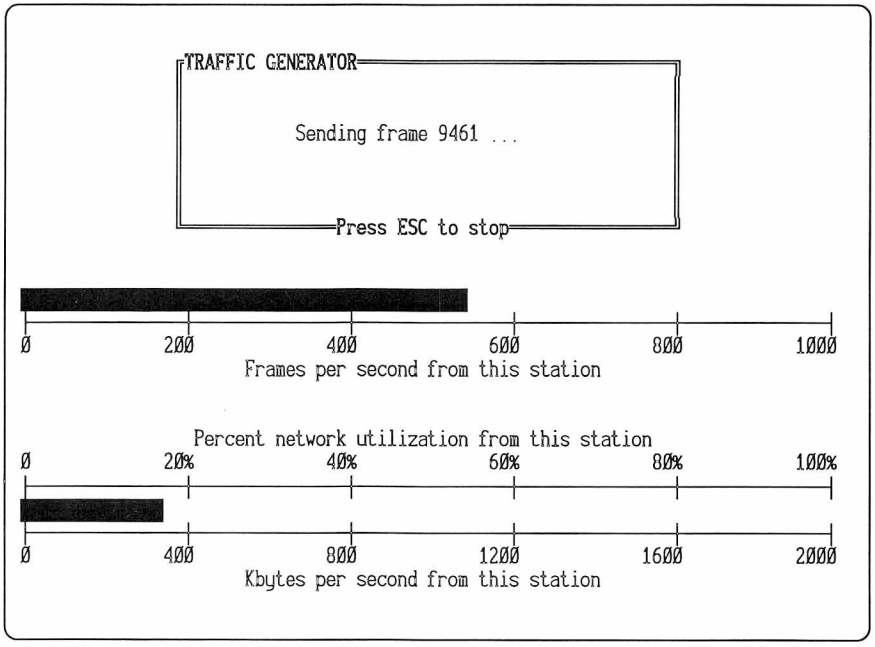


Figure 10–8. Generating frames on a token ring network

NOTE: While the Sniffer analyzer generates traffic, it does not perform any other Sniffer functions. However, on a token ring network, the Sniffer analyzer can be the

"active monitor" for the ring as it continues to forward incoming frames from its upstream neighbor.

To stop the Traffic generator:

1. Press ESC.

Example: Format of the Generated Frame

The generated frame's format depends on the network. Figure 10–9 shows how a frame to be generated in **Single Frame mode** was defined. Figure 10–10 shows how that frame appears when captured by another analyzer. (On a different network, the frame would differ slightly.)

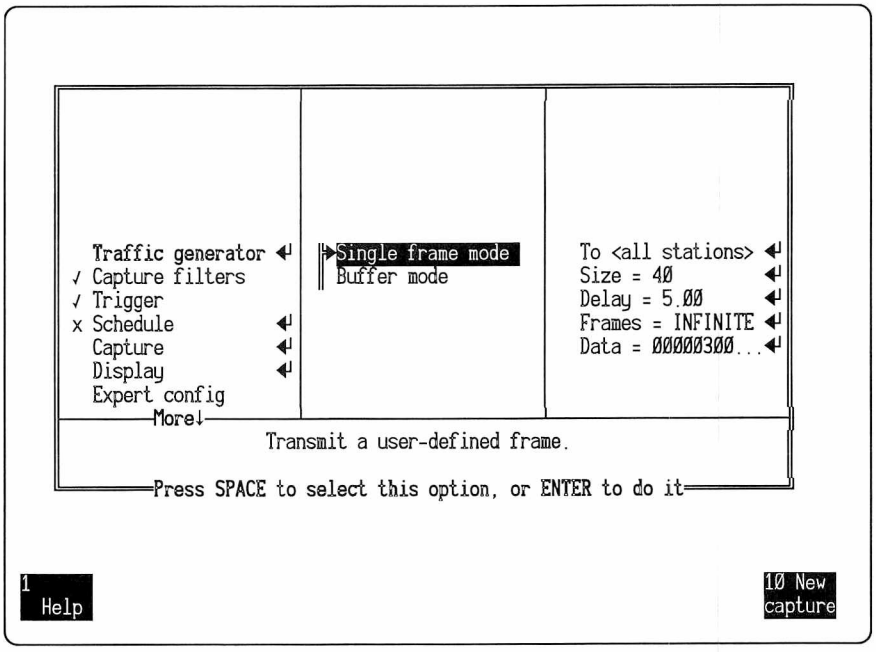


Figure 10–9. Defining a token ring frame to be generated

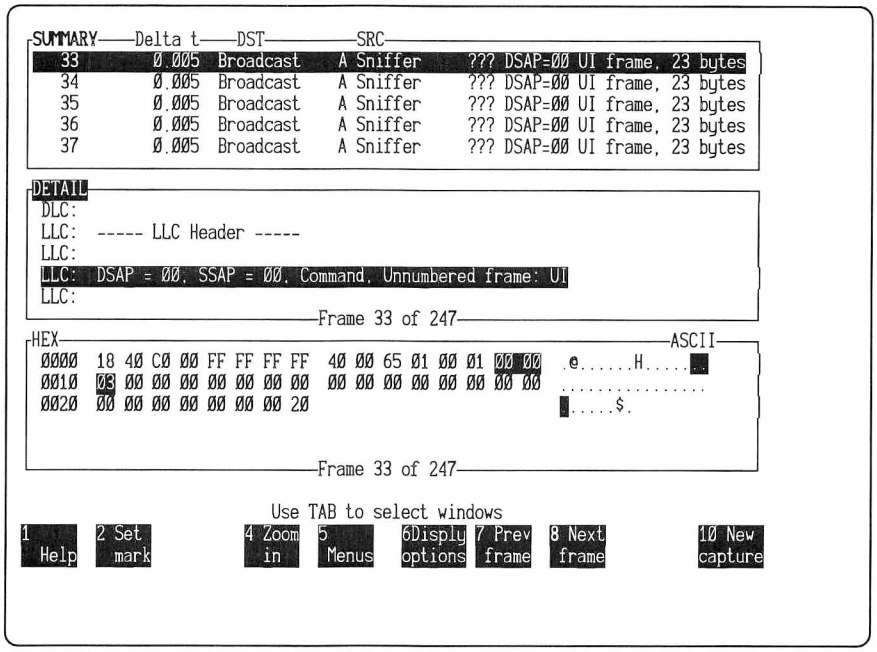

SUMMARY Delta t DST SRC
33 Ø.ØØ5 Broadcast A Sniffer ??? DSAP=ØØ UI frame, 23 bytes
34 Ø.ØØ5 Broadcast A Sniffer ??? DSAP=ØØ UI frame, 23 bytes
35 Ø.ØØ5 Broadcast A Sniffer ??? DSAP=ØØ UI frame, 23 bytes
36 Ø.ØØ5 Broadcast A Sniffer ??? DSAP=ØØ UI frame, 23 bytes
37 Ø.ØØ5 Broadcast A Sniffer ??? DSAP=ØØ UI frame, 23 bytes
DETAIL
DLC:
LLC: ----- LLC Header -----
LLC:
LLC: DSAP = ØØ, SSAP = ØØ, Command, Unnumbered frame: UI
LLC:
Frame 33 of 247
HEX ASCII
ØØØØ 18 4Ø CØ ØØ FF FF FF FF 4Ø ØØ 65 Ø1 ØØ Ø1 ØØ ØØ .@.....H.....
ØØ1Ø ØØ ØØ ØØ ØØ ØØ ØØ ØØ ØØ ØØ ØØ ØØ ØØ ØØ ØØ ØØ ....
ØØ2Ø ØØ ØØ ØØ ØØ ØØ ØØ ØØ 2Ø .....$.
Frame 33 of 247
Use TAB to select windows
1 Help
2 Set mark
4 Zoom in
5 Menus
6Disply options
7 Prev frame
8 Next frame
10 New capture

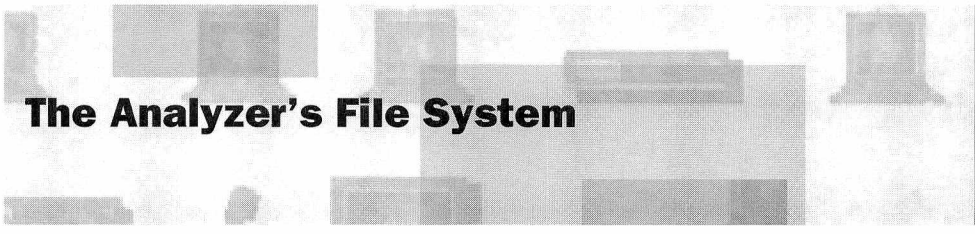
Figure 10–10. Appearance of the generated token ring frame

As shown above, each generated frame consists of the following information:

- The first two bytes are the AC and FC bytes of the standard DLC header, visible in the Hex view as the characters 18 40.
- The next six bytes are the destination address (in this case, C0 00 FF FF FF FF, which means "Broadcast").
- The next six bytes are the source address (in this example, 40 00 65 01 00 01, which is the address of the Sniffer Network Analyzer that generated the frame).
- The next 32 bytes contain the data specified for the data field, starting with 00 00 03 00 ... 00. (On token ring, this default remains in effect unless you enter other values for the data field.) Following the standard header and whatever bytes you specify for the data field, the remainder of the frame consists of as many repetitions of 00 (hex) as necessary to create the total size you requested.
- The last four bytes show the sequence number 00 20.

In the Detail view, which shows the interpreted frame, the DSAP and SSAP fields are both 00. Since those values do not match any protocol known to the Sniffer analyzer, it shows the protocol as "???". The analyzer interprets the first 4 bytes as UI and attaches the explanatory text "Unnumbered information."

In the Hex view, the first three of those four bytes are highlighted. (The fourth is not highlighted because the preceding bytes are sufficient to identify the UI command, and the protocol interpreter knows that UI makes no use of the fourth byte.)



The Analyzer's File System

11

The Analyzer's File System

Overview

During everyday use of the Sniffer Network Analyzer, you should not need the information in this chapter. However, knowledge of the system files may prove useful for a general understanding, as well as for importing and exporting files.

This chapter describes:

- The use of file names and extensions
- Files that the Sniffer analyzer uses and the directories that contain them
- Procedures for working with these files
- The file formats used to store name tables, setups, and saved data
- The analyzer's parameters

About File Names and Extensions

With DOS, a file's name consists of two parts, separated by a dot. The first part (base name) may contain up to eight characters. The second part (extension) consists of three letters. Certain extensions have special significance to DOS. For example, all executable files have the extension .EXE, .COM, or .BAT—DOS won't execute a file with another extension. Other extensions identify a file's use or the type of data in the file. Figure 11–1 summarizes these extensions.

Extension	File type
.EXE	Executable file. This extension may be omitted from the command that invokes its execution.
.BAT	Batch file, which is an executable file that consists of commands in the DOS shell language. The extension may be omitted from the command that invokes its execution.
.PRN	Output file generated for printing, directed either to a printer or to a file.
.CSV	Output file generated as "comma separated values," used to import or export data.
.TXT	Script that generates the menus, used by the executable MENUX.EXE.
.MNU	Script used to generate a particular analyzer entry in the menu.
.CFG	Configuration file that specifies the protocol interpreters for a particular network or specifies scheduled events.
.HLP	File that contains online help information for the Sniffer Network Analyzer.

Figure 11–1. General DOS extensions

Each of the executable files is specific to a single network, as indicated by an extension that identifies the network (first two letters) and the type of file (last letter), as shown in Figure 11–2. For example, if you save frames captured on an Ethernet network to a file called MYDATA, the Sniffer analyzer assigns the extension .ENC, resulting in the file MYDATA.ENC.

First two letters	Type of network
EN	Ethernet and Ethernet-II
TR	Token Ring
FD	FDDI
SY	WAN/Synchronous
AR	ARCNET
LT	LocalTalk
SL	StarLAN
PC	PC Network
Last letter	**Type of file**
C	Captured frames
S	Setup values used to define various system options
D	Station names, the symbolic equivalents for numeric addresses
I	Manufacturer IDs, the symbolic equivalents for the manufacturer codes within numeric addresses
B	Binary type, used only by the Sniffer Monitor application
V	Expert configuration data

Figure 11–2. Sniffer analyzer extensions

The Sniffer Analyzer Directories and Files

Figure 11–3 summarizes the Sniffer analyzer directories for the analyzer on the hard disk (drive C).

Directory	Files
DOS operating system	Required DOS files
TOOLS	Miscellaneous utility programs
CONFIG	The files that list the facilities available to the Sniffer
xxSNIFF	Monitor executable files Analyzer executable files Setup files, including STARTUP.*xx*S Configuration files Help files
xxREPORT	Expert data files in .CSV format
CAPTURE	Files of captured frames (trace files) Output files .PRN, non-expert .CSV The help configuration file (HELP.ENV)
REMOTE2	Required DCA Remote2 files, used for remote operation

Figure 11–3. The Sniffer analyzer directories

Root Directory

The root directory contains the files AUTOEXEC.BAT and CONFIG.SYS. The system refers to them automatically each time you reboot or restart following a power-down.

The AUTOEXEC.BAT file establishes the path: that is, the list of directories in which the operating system searches for executable files. This file also invokes the main selection menu. From there, you select which of the programs you want to use (DCA Remote2, Monitor or Analyzer).

DOS Directory

The DOS directory contains the files that belong to the operating system (except for the few DOS files that are in the root directory). The path includes the DOS directory, which the operating system uses to find its own files. Normally, you will not need to change any files in the DOS directory.

TOOLS Directory

The TOOLS directory contains various utilities. The DOS path directs the operating system to the \TOOLS directory, so you will not usually need to make any explicit reference to it.

CONFIG Directory

The CONFIG directory contains the files that generate the main selection menu and the analyzer's main menu.

*xx*SNIFF Directory

This directory contains the principal executable files, both for the Sniffer monitor and for the various Sniffer analyzer configurations. The directory's name is formed from the two-letter network abbreviation, followed by the letters SNIFF, such as TRSNIFF for token ring. The analyzer contains only the directories appropriate for your network.

Files and Subdirectories within the xxSNIFF Directory

Each executable file is accompanied by a menu file with the same base name, but with the extension .MNU rather than .EXE. The executable files reside in the xxSNIFF directory (that is, ENSNIFF, FDSNIFF, or TRSNIFF). However, all .MNU files reside in the \CONFIG directory.

The analyzer uses the various menu files to generate entries in the main selection menu. Each menu file is responsible for the menu entry corresponding to one Sniffer analyzer or monitor. The .EXE files and the .MNU files are already supplied by Network General. In addition to the Monitor and Analyzer executable files, the xxSNIFF directory contains the following files and subdirectories:

- STARTUP.xxD: Contains the name table with all addresses and associated symbolic names. For more information about the STARTUP files, see "STARTUP Files" on page 11–10.
- STARTUP.xxI: Contains the table of the manufacturers' IDs.
- SETUP files, including STARTUP.*xx*S.
- DEFAULTS.xxS: Contains the factory default values for various options, such as filters, triggers, and screen formats.

IMPORTANT: Do not alter DEFAULTS.xxS.

- HELP subdirectory: Contains the files that generate the analyzer and monitor help systems, which are displayed when the user presses F1 **[Help]**.

- XPHELP subdirectory. Contains the Expert explain files.
- xxSNIFF.CFG subdirectory: Lists the facilities available to the Sniffer Network Analyzer and encodes all the protocol interpreter suites that can be installed. **NOTE:** xxSNIFF.CFG is a binary file—do not alter it.

*xx*REPORT Directory

This directory contains the Expert data files that are saved by the Event Scheduler in CSV format. Each of these files has a .CSV extension, and a file name based on the date and time at which the file is saved.

CAPTURE Directory

The \CAPTURE directory contains the files that contain captured frames (trace files). It is also the default destination for .PRN output files and non-expert .CSV files.

For trace files, you assign the filename and the analyzer automatically assigns a three-letter extension. The first two letters identify the network (as shown in Figure 11–2), and the last letter is C, which identifies the file as a trace file that contains captured frames.

Trace files have the same internal format as the capture buffer. You cannot read a capture file as text.

REMOTE2 Directory

The REMOTE2 directory contains the files used for remote operation of the Sniffer analyzer.

Configuring the Remote^2 Host

To configure Remote^2 to answer calls from a remote Sniffer Network Analyzer, you must have a System Manager password. Network General provides Remote^2 Manager with the following default System Manager ID and password:

Default System Manager ID: `MANAGER`

Default System Manager Password: `MANAGER`

To configure Remote² Host to answer calls from a remote Sniffer Network Analyzer:

1. From the Main Selection Menu of the Sniffer Network Analyzer, highlight **DCA Remote²** and press ENTER.
   Result: The **TeleSniffer Selection Menu for Remote²** appears.
2. Highlight **Configure Sniffer Host** and press ENTER.
   Result: The Remote² Manager prompts for a User ID and password.
3. Type in the default System Manager ID and password as provided by Network General.
   Result: The main menu of the Remote² Manager appears. From here, you can decide on the Remote² Host operating configuration and set up or change the operating parameters for Remote² Host users. For more information on the Remote² Manager, see the *DCA Remote2 Supplement*, provided with your Sniffer Network Analyzer.
   NOTE: You can use the Remote² Manager to change the default password.

Working with Files

Creating Alternate Directories for Saved Files

To keep your trace files organized, you may want to set up directories in addition to the default directory \CAPTURE.

To create a new directory:

1. Move to **Files\Make directory** and press ENTER.
   The Sniffer analyzer opens a dialog box to receive the name of the new directory. The analyzer displays the current path, which is C:\CAPTURE\, unless you previously changed the path.
2. Type the new directory name to the right of the final \ to create a subdirectory of \CAPTURE. You can also backspace over all or part of the path and replace it with whatever you prefer. Press ENTER to record the name and create the directory. Do not specify an extension.

IMPORTANT: Because the Sniffer analyzer limits the file name to eight alphabetic characters, you cannot specify an extension for a directory created in this way. If you write a longer name, it is truncated to the first eight characters.

The analyzer accepts the path you specify without verifying that it is syntactically valid or that the directory actually exists. If the path is not valid, you will get the error message "Invalid path" when you subsequently try to read or write a file.

Setting the Path to a Directory for Saved Files

All dialog boxes that let you select an existing file or enter a filename for a new file show the path to the current directory. Initially, this path is C:\CAPTURE\.

To specify the initial path to saved files:

1. Move to **Files\Change path** and press ENTER.
2. In the dialog box that appears, type the desired path and press ENTER. The path should start with a subdirectory and end with a \ character. As a result, all dialog boxes that are displayed will specify the path you defined.

   Specify a drive and directory. For example, instead of specifying, "A:\" as the new path, specify, "A:\CAPTURE," or another directory name.

NOTE: The analyzer accepts the path you specify without verifying that it is syntactically valid or that the directory actually exists. If the path is not valid, you will get the error message "Invalid path" when you subsequently try to read or write a file.

STARTUP Files

For information about names associated with addresses or about setups of user-defined options, the Sniffer analyzer refers to four kinds of files, which are identified by the last letter of the extension. Each time the analyzer executes, it refers to one or more of these files. Figure 11–4 lists the various startup files.

File name	Contains	How used
STARTUP.xxD	Symbolic names for addresses	At startup, it builds the working name table by reading \xxSNIFF\STARTUP.xxD.
STARTUP.xxI	Symbolic names for manufacturer IDs	At startup, it reads the table of manufacturer IDs from \xxSNIFF\STARTUP.xxI.
STARTUP.xxS	Values for setups of user-defined options.	At startup, it reads from \CAPTURE\STARTUP.xxS to determine values for various options such as filters. This file is user-definable; any options saved with this file name will be automatically applied at startup.
STARTUP.xxV	Values for Expert options	At startup, it reads the Expert configuration for subnet masks and trustee names.
SCHEDULE.CFG	Scheduled events	At startup, it reads from C:\CAPTURE\SCHEDULE.CFG to determine what scheduled events to run and when to run them.

Figure 11–4. The Sniffer analyzer startup files

Each time you start the analyzer, the software automatically checks for the startup files in the *xx*SNIFF and \CAPTURE directories. If it finds them, it uses them to set its working name table, or to initialize the Sniffer analyzer's filters and settings.

The three types of files (name files, manufacturer ID files, and setup or startup files) use different mechanisms for loading and saving, as shown in Figure 11–5.

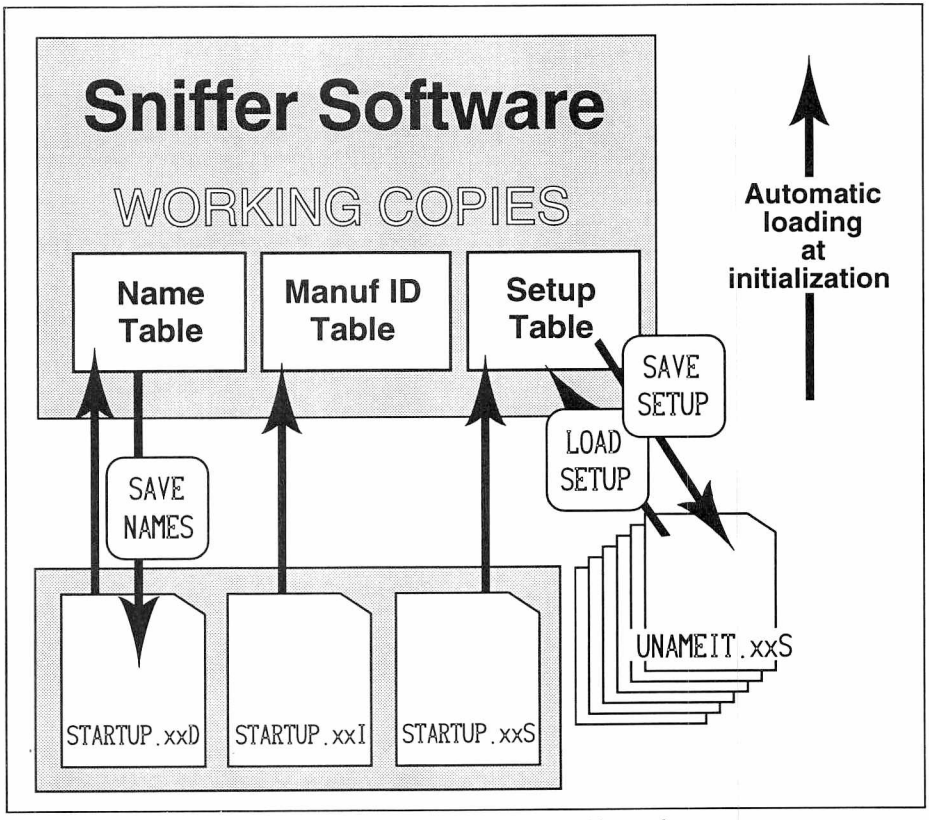


Figure 11–5. Stored files and working copies of name tables and setups

Modifying the STARTUP.xxS File

The STARTUP.xxS file determines which settings and options are applied at startup. The Sniffer analyzer does not require a startup file. When the analyzer starts, it checks to see whether a STARTUP.*xx*S file exists.

- If the file exists, the analyzer uses it.
- If the file does not exist, the analyzer uses the default values coded into the Sniffer analyzer executable.

To define the startup options:

1. Define all options as desired.
2. Move to **Files \ Save \ Setups** and press ENTER.

3. In the dialog box that appears, type STARTUP. The resulting path will be as follows:

   C:\xxSNIFF\STARTUP

   Don't include an extension; the Sniffer analyzer automatically attaches the extension .*xx*S (where *xx* is the two-letter network abbreviation). A warning dialog box appears. You can either abort the request or overwrite the existing file.

Restoring the Factory Defaults

If you have used a customized setup and want to revert to a known state, you can reapply the analyzer's default setup.

To restore the factory defaults:

1. Move to **Options\Use defaults** and press ENTER.

About the Name Tables

Procedures for assigning names to stations are described in Chapter 8, starting on page 8–6. This section describes the format of files that contain name tables.

While it runs, the analyzer uses an internal directory called the *working name table*. Each time you start the analyzer thereafter, it initializes the working name table by reading from a file. Ordinarily, the file it reads is *xx*SNIFF\STARTUP.*xx*D.

If the Sniffer analyzer cannot find *xx*SNIFF\STARTUP.*xx*D, it looks in the current directory (that is, the directory identified by the **Change path** command).

If it does not find that file, the analyzer sets up an empty name table, containing only the address of the adapter card and the name "This Sniffer."

You may have additional reference files of names and station addresses. These are either renamed copies of what was once a STARTUP.*xx*D file, or files in the same format created by an editor and loaded in the Sniffer analyzer. When you create such a file, you must name it something other than STARTUP, although it will have the same extension as a startup file.

You can read from these additional name files by executing the **Resolve names** command (see page 8–9).

The extra name files are used as a source of names to fill blanks in the working name table. There is no command to load an entire substitute name file, the way you load a setup. If you want to maintain several independent name files, use the DOS commands to give them arbitrary names. Before you start the Sniffer analyzer, assign

a new name to your existing file STARTUP.*xx*D, and then copy the file you want to make active and name it STARTUP.*xx*D.

Creating Name Files

A name file is identified by an extension consisting of the two-letter network code followed by the letter "D". There are two principal ways to create a name file: by saving and then renaming the working name table, and by writing a name file from scratch with a text editor.

To create a name file from the current working name table:

1. Move to **Display\Manage names\Edit names** and press ENTER.
2. Edit the name table that appears, as described in "To edit the working name table:" on page 8–7. When you are finished, press ESC to return to the menus.
3. Move to **Save names** and press ENTER. The Sniffer analyzer saves a file called *xx*SNIFF\STARTUP.*xx*D, which contains names and addresses for all named stations. Any stations that are not named are discarded.
4. Move to **Exit** and press ENTER. Move to **Return to DOS** and press ENTER.
5. At the DOS prompt, copy and rename the file as follows:
   COPY *xx*SNIFF\STARTUP.*xx*D \CAPTURE*newname*.*

Creating Your Own Name File

You can create your own name file directly. This section describes a name file's internal format.

All name files have the same format, which applies both to the file called STARTUP.*xx*D and any other name files you may use as sources. Figure 11–6 shows part of a name file. Since a name file is a standard ASCII file, you can build it on the Sniffer analyzer or any other PC, using any standard text editor.

```
station "Broadcast"     = addrtype "DLC" C000FFFFFFFF
station "Error Log"     = addrtype "DLC" C000000000008
station "ipS1"          = addrtype "IP" [36.10.0.13]
station "ipS2"          = addrtype "IP" [36.11.0.14]
station "ipS3"          = addrtype "IP" [36.11.0.23]
station "ipS4"          = addrtype "IP" [36.2.0.5]
station "ipS5"          = addrtype "IP" [36.22.0.20]
station "Long, 31-Character Station Name" = addrtype "DLC" 400000000002
station "Mary"          = addrtype "DLC" 10005A0033BF
station "This Sniffer"  = addrtype "DLC" 48000A000001
station "Tom"           = addrtype "DLC" 10005A002FEB
station "Faquard"       = addrtype "XNS" 08000AC7CEFE
```

Figure 11–6. Sample name file

The **Save names** command sorts the rows of the table alphabetically by name. However, the analyzer does not require a name file to be in alphabetical order.

The following features of a name table are illustrated in Figure 11–6 and Figure 11–7.

Type

Each line starts with a word or symbol that identifies its type. The three line types are distinguished by the following as their first non-blank characters:

`station`	The balance of the line describes one station's name and address.
`addrtype`	The balance of the line sets the default address type (protocol) that applies to subsequent lines that don't include it explicitly.
`/*`	A line that starts with /* and ends with */ is a comment and is not executed.

Name

The station's name appears to the right of the word "station." The name must be enclosed in double quotes.

Address type

Each address must be assigned to a specific type (that is, protocol). The type can be stated in either of two ways:

- Explicitly for each address, by including the phrase `addrtype "DLC"` to the left of the address (as shown in Figure 11–6). A name file generated by the **Save names** command is entirely in this form.
- Implicitly, using the current default type (Figure 11–7). An address that has no explicit type is presumed to belong to the current default type. The default type is initially "DLC". The default type is set by each use of **addrtype**, and remains in effect until another **addrtype**.

Address

There is an = sign between the name and the address. An address is not enclosed in quotes. Each address is written in a form appropriate to its type (the same way the Sniffer displays it in the detail view). For example, a 6-byte DLC address is written as 12 hexadecimal digits. A 4-byte IP address is written as four decimal numbers separated by dots and surrounded by square brackets.

Name Table with Default Types

Figure 11–7 shows the same information as Figure 11–6, but makes use of *default types*. To improve readability, the file may contain redundant blanks or blank lines, as well as comments. A comment starts with /* and ends with */.

```
 station "Error Log" = C00000000008
addrtype "IP"
 station "ipS1" = [36.10.0.13]
 station "ipS2" = [36.11.0.14]
 station "ipS3" = [36.11.0.23]
 station "ipS4" = [36.2.0.5]
 station "ipS5" = [36.22.0.20]
 station "ipS6" = [36.26.0.54]
 station "ipS7" = [36.26.0.56]
addrtype "DLC"
/* Long name inserted as a test */
 station "Long, 31-Character Station Name"=400000000002
 station "Mary" = 10005A0033BF
 station "This Sniffer" = 48000A000001
 station "Tom" = 10005A002FEB
addrtype "XNS"
 station "Faquard" = 08000AC7CEFE
```

Figure 11–7. The name file of Figure 11–6 rewritten with default types

Alphabetization of Station Names

You can enter names in any order. When the Sniffer builds and displays its working name table, it shows the list in alphabetical order by name. Addresses that you have not named (and therefore have blank names) appear at the top of the list.

Each time you edit the working name table, the Sniffer re-alphabetizes the list. When you execute **Save names**, the saved file preserves the alphabetical order of the working name table. However, entries that are not named are discarded.

Table of Manufacturer ID Codes and Abbreviations

On most LANs, an address consists of six bytes. If you enabled the **Manufacturers IDs** option, the Sniffer represents the first three bytes of the address with a six-character abbreviation of the manufacturer's name. It follows the abbreviation with six hexadecimal characters—for example, Intrln031EF7.

The table of manufacturer codes and names is located in the file startup.*xx*I, where *xx* is the two-letter code for the network, and I indicates the ID table. The file's internal format is illustrated in Figure 11–8. The figure shows the content of the file STARTUP.*xx*I for a network that transmits least significant bit first (for example, Ethernet but not token ring). The comments in the file are for the convenience of the user and have no effect on the Sniffer analyzer's use of the file. (For compactness, the

lower part of the table is shown here with three entries per line. In the file, each entry has a line of its own.)

```
/* Sniffer table of assigned manufacturer IDs.                          */
/*                                                                      */
/* This is for networks where the LSB is sent first, such as            */
/* Ethernet, StarLAN, and PC Network. Note that we've put in here       */
/* what we actually see in the real world, not what IEEE would like     */
/*                                                                      */
manuf "VisTec" = 000022 /* Visual Technology, Inc.                      */
manuf "NwkGnl" = 000065 /* Network General Corp.                        */
manuf "Prteon" = 000093 /* Proteon (bit-reversed from token ring!)      */
manuf "Amrstr" = 00009f /* Ameristar Technology                         */
manuf "Wllflt" = 0000a2 /* Wellfleet                                    */
manuf "NCD "   = 0000a7 /* Network Computing Devices, Inc.              */
manuf "NSC "   = 0000a9 /* Network Systems Corp.                        */
manuf "RND "   = 0000b0 /* RAD Network Devices Ltd.                     */
manuf "Cimlin" = 0000b3 /* CIMlinc                                      */
manuf "WstDig" = 0000c0 /* Western Digital                              */
manuf "HP EON" = 0000c6 /* H-P Intlgnt Networks Oper (EON)              */
manuf "IBM "   = 10005a /* (not bit-reversed from token ring)           */
manuf "Intrln" = 020701 /* Interlan, Inc.                               */
manuf "NSC "   = 080017 /* Network System Corp.                         */
manuf "Intrgr" = 080036 /* Intergraph                                   */
manuf "Univtn" = 080049 /* Univation                                    */
manuf "IBM "   = 08005a /* (bit-reversed from token ring)               */
manuf "ComDes" = 080067 /* ComDesign                                    */

manuf "Xerox " = 0000aa
manuf "Dove "  = 0000b7
manuf "MIPS "  = 00006b
manuf "Ardent" = 00007a
manuf "Cayman" = 000089
manuf "TRW "   = 00002a
manuf "Cisco " = 00000c
manuf "NeXT "  = 00000f
manuf "Sytek " = 000010
manuf "Novell" = 00001b
manuf "Altos " = 0000c8
manuf "Could " = 0000dd
manuf "Acer "  = 0000e2
manuf "Alantc" = 0000ef
manuf "Agilis" = 00805c
manuf "Intel " = 00aa00
manuf "U-B "   = 00dd00
manuf "U-B "   = 00dd01
manuf "3Com "  = 02608c
manuf "CMC "   = 02cf1f
manuf "Bridge" = 080002

manuf "ACC "   = 080003
manuf "Symblx" = 080005
manuf "Apple " = 080007
manuf "BBN "   = 080008
manuf "H-P "   = 080009
manuf "Nestar" = 08000a
manuf "Unisys" = 08000b
manuf "AT&T "  = 080010
manuf "Tktrnx" = 080011
manuf "Exceln" = 080014
manuf "DG "    = 08001a

manuf "DG "    = 08001b
manuf "Apollo" = 08001e
manuf "Sun "   = 080020
manuf "NBI "   = 080022
manuf "CDC "   = 080025
manuf "TI "    = 080028
manuf "DECnet" = 08002b
manuf "Mtaphr" = 08002e
manuf "Spider" = 080039
manuf "DCA "   = 080041
manuf "Sequnt" = 080047
manuf "Encore" = 08004c
manuf "BICC "  = 08004e
manuf "Ridge " = 080068
manuf "SGL" = 080069
manuf "AT&T "  = 08006a
manuf "Exceln" = 08006e
manuf "Vtalnk" = 08007c
manuf "Xyplex" = 080087
manuf "Kinetx" = 080089
manuf "Pyramd" = 08008b
```

Figure 11–8. Manufacturer ID translation

Manufacturer IDs in the table are shown as they appear in the computer once they have been captured. The IEEE assignment of IDs specifies the sequence in which bits are transmitted on the wire. For networks that transmit each byte low-order-bit first (such as Ethernet) the address you see after it has been captured is the byte-by-byte reverse of what was transmitted on the wire. For example, the code used by IBM is transmitted on the network by the sequence 00010000 00000000 01011010. It

appears to a token ring Sniffer analyzer as 10 00 5A, but to an Ethernet Sniffer analyzer as 08 00 5A.

File Formats

The contents of the capture buffer (before or after filtering) may be saved in a file or sent to a printer. If saved in a file, the contents may be in a printer format (with or without page titles and page numbers), or in the CSV format recognized by standard spreadsheets. The files thus produced have the extension .PRN for printer files and .CSV for spreadsheet files. (For details of this procedure, see, "To create a report:" on page 7–62.)

This document does not describe the format of the Expert analyzer's CSV output file. For a full description of the file format for the Expert Analyzer output file, see the accompanying document, *Expert Analyzer Output File Format.*

Format of Saved Data Files

You can use a saved data file for data analysis. For example, you can write a program that reads through a file of saved frames. The easiest format to work with is the ASCII file you get when you "print" the capture buffer to a file. This can be especially helpful if you choose the option to omit page titles. The resulting file will contain the information you want in an easily-accessible format.

Alternatively, you may prefer to operate directly on the trace file the analyzer writes in response to the **Save data** command. This section describes the format of such a trace file.

Each trace file consists of sequences of variable length binary records. Since all 256 byte values are possible within the data, you cannot edit this file using an ordinary text editor.

The first 16 bytes of a trace file contain a text message identifying the file as one containing data collected by the analyzer.[1] The message is followed by an end-of-file character (hex 1A, also called CTRL-Z). Even if you accidentally type the file to the screen, or otherwise treat it as a text file, the display reaches a terminator before reaching unprintable characters.

IMPORTANT: You must save the file uncompressed to use this format specification.

1. The message in these files is "TRSNIFF data," no matter where the frames were collected.

Structures within the Data File

Following the text message string, the file contains an arbitrary number of variable-length records. Each record has a type, identified in its first two bytes. The three principal types are:

- Version record
- Frame record
- End-of-file record

The first record in the file is always a version record, the last is always an end-of-file record, and those in between are usually (but not necessarily) frame records.

There is no explicit encoding of the file's total length (except as part of its directory entry).

Header

Every record of any type begins with the following header:

```
struct f_rec_struc {    /* Standard record header.                    */
int    type;            /* Type of this record. (Int = 2 bytes)       */
int    length;          /* Length of remainder of this record.        */
int    rsvd;            /* Reserved word, currently Ø.                */
};
```

The header's first field indicates what type of record follows. The three principal types are identified by the following values:

```
#define REC_VERS          1    /* Version record (f_vers).           */
#define REC_FRAME2        4    /* Frame data (f_frame2).             */
#define REC_EOF           3    /* End-of-file record (no data follows). */
```

Types other than these are reserved for future or other use. If you write a program to process data files, you should have it skip any record that is not one of these types. The length field indicates how much data to skip.

Format of a Version Record

```
struct f_vers_struct   {
int        maj_vers;          /* Major version of the Sniffer       */
int        min_vers;          /* Minor version of the Sniffer       */
struct     date_struct date   /* Date & time (4 bytes, DOS format[1]) */
```

1. Standard DOS format for dates is *mm-dd-yy*. Standard DOS format for times is *hh:mm*, followed by a one-letter designation for AM/PM.

```
char      type;          /* What type of records follow.          */
char      network;       /* An indicator of the network type.     */
char      format;        /* An indicator of the format version.   */
char      timeunit;      /* An indicator of the frame timestamp unit. */
int       rsvd[3];       /* Reserved words.                       */
};
```

Here are the possible values of **network** are as follows:

```
#define       NETWORK_TRING          0    /* Token ring          */
#define       NETWORK_ENET           1    /* Ethernet            */
#define       NETWORK_ARCNET         2    /* ARCNET              */
#define       NETWORK_STARLAN        3    /* StarLAN             */
#define       NETWORK_PCNW           4    /* PC Network broadband */
#define       NETWORK_LOCALTALK      5    /* LocalTalk           */
#define       NETWORK_FDDI           9    /* FDDI                */
#define       NETWORK_SYNCHRO        7    /* Internetwork analyzer */
```

The possible values of **timeunit** are as follows:

```
#define  TIMEUNIT_UNSPEC   0  /*  Unspecified; default by network type. */
#define  TIMEUNIT_PC       1  /*   0.838096       microsecond units    */
#define  TIMEUNIT_3COM     2  /*  15.000000       microsecond units    */
#define  TIMEUNIT_NPI      3  /*   0.088000       microsecond units    */
#define  TIMEUNIT_SYTEK    4  /*   2.000000       microsecond units    */
```

Madge and Cogent cards use TIMEUNIT_PC.

Format of a Frame Data Record

Each record starts with a header, as described above, followed by data in the following structure:

```
struct    f_frame2_struct     {
unsigned  time_low;       /* Low time, network-dependent units.        */
unsigned  time_mid;       /* Mid time, network-dependent units.        */
char      time_high;      /* High time, network-dependent units.       */
char      time_day;       /* Time in days since start of capture.      */
int       size;           /* Number of bytes actually written in this file
                             (may be less than frame's original length).  */
char      fs;             /* Frame error status bits.                  */
char      flags;          /* Buffer flags; for internal use.           */
int       true_size;      /* If nonzero, the size of the original frame
                             (since this frame has been truncated).    */
int       rsvd;   }       /* Reserved; currently 0.
                             The frame data follows.                   */
```

All multibyte arithmetic fields (computed by the analyzer during capture) are stored with the least significant byte first. Frame data are stored in the byte order transmitted.

Format of an End-of-file Record

The end-of-file record has no data; it consists only of the record header.

The Startup Parameters

A number of parameters affect the analyzer's operation. Some parameters reflect the particular platform and network interface card, so they should not be changed. Others reflect the way you use the analyzer, which may change with circumstances. For those parameters that are likely to change, there are items in the menu. The following sections describe how to alter the **Automatic Restart** option, which is located in the main selection menu, and how to alter software parameters that are not represented in the menus.

WARNING. In many cases, if you change a startup parameter you must also change the physical equipment. For example, if you change the software record of parameters like the NIC's interrupt request, you must also change the appropriate jumpers or dip switches on the interface card.

These kinds of changes are probably necessary only when you introduce non-standard variations in the equipment you are using. Network General does not recommend that you make these kinds of changes. Before you change the Sniffer analyzer's hardware, consult the Technical Support Department at Network General Corporation.

Automatic Restart Option

You can choose whether or not the analyzer will automatically restart a capture session if there is a power failure during the session. (This feature is not available in the Notebook Sniffer Analyzer.)

To enable the **Automatic Restart** option, move to the **Enable Automatic Restart** option in the main selection menu and press the Spacebar to enable it. When you have enabled the **Automatic Restart** option, the main selection menu will show **Disable Automatic Restart**; to disable the function, move to **Disable Automatic Restart** and press the Spacebar.

How the Parameters are Passed

The statement that launches the Sniffer analyzer receives input from two sources. Depending on the change you want, there are two places you can change the files. This section describes the files you can change.

The command to launch a Sniffer analyzer is located inside the batch file that executes when you select an analyzer in the main selection menu and press ENTER.

When you select an analyzer in the main selection menu and press ENTER, you invoke the file xxSNIFF.MNU. That file invokes SNGO.xx, which calls xxPARAM.BAT and invokes SNGO2.xx. The file SNGO2.xx invokes SNSTART, which invokes SNLOAD, which starts the Sniffer Network Analyzer.

The file SNSTART.BAT does not contain the startup parameters. It receives them as arguments, or by referring to DOS environment variables. Each application listed in the main selection menu has a configuration file \xxSNIFF\xxPARAM.BAT which specifies the arguments that will be passed to SNSTART.BAT.

Thus, to change one analyzer, edit its xxPARAM.BAT file (as described in the procedure below).

Here is a sample ENPARAM.BAT file:

```
@echo off
set param="RAMBASE:D400 MAXSTNS:800"
set mem=i:d800-dfff
```

Editing the Startup Parameters

You can edit the startup parameters in the following ways.

To edit the startup parameters:

- If you want to modify parameters for a specific analyzer, edit its xxPARAM.BAT file.

  Locate the file \xxSNIFF\xxPARAM.BAT. In its `set param=` line, replace the characters `nop` with one or more parameters, each set off by blanks. (You may place up to 70 characters between the quotation marks.)

  For example, if you specify a maximum of 800 names in the address table, replace `nop` with `maxstns:800`.

  Before: `set param="NOP"`
  After: `Set param= "maxstns:800"`

  NOTE: If you increase the maximum number of stations to more than 5000 names, and your network is heavily loaded, and you want to use the **Look for names** and **Edit names** functions, use the following precaution:

Do not use the **Look for names** and **Edit names** features after displaying analyzed data. If you need to edit, save the file and then reload it. Do not display it now—use **Edit names** to change the name table, then display it.

NOTE: Do not modify the `mem:` line unless you need to exclude a specific portion of memory—typically when you add a device to your machine that uses a specific portion of memory for its BIOS.

- If you want to set screen parameters, set the appropriate DOS environment variables.

  You can use DOS environment variables to set values for SCR (which specifies the type of monitor) or SCRMODE (which controls the way the scrolling is shown as you move from one menu panel to another). At the DOS prompt, type `set scr=` or `set scrmode=` followed by one of the possible values.

WARNING. The Sniffer loses its environment variables when you reset the machine or turn off power. To automatically regenerate them at power-up, insert a statement in \AUTOEXEC.BAT. Choosing any of the screen options in the main selection menu also sets the environment variable SCR (and therefore overwrites any earlier setting of SCR).

Startup Parameters List

The tables that follow show the parameters for which you can define values. Figure 11–9 shows the startup parameters that affect the context of use, Figure 11–10 shows the parameters that affect expanded memory, and Figure 11–11 shows the startup parameters that report the configuration of the adapter card.

Parameter	Values
Screen display attributes (DOS environment variable SCR). To optimize attributes in the analyzer's display screens, the analyzer selects color or shading attributes to match the capabilities of various devices. GRAY is intended for Compaq monochrome gray scale, LCD for liquid crystal displays with black characters on a clear background, and LCDR for the reverse.	MONO COLOR/COLOUR GRAY/GREY LCD LCDR PLASMA
Scrolling during panel-to-panel movement (DOS environment variable SCR mode). On a local screen during transition to a new panel, the analyzer redraws the screen in stages to convey the effect of motion. When you control the analyzer from a remote station, it may be preferable to eliminate the transition display to save time.	NOSCROLL
Typeahead By default, the analyzer does not accept new keystrokes during display. You may permit typeahead up to the limit of the DOS input buffer (15 characters).	TYPEAHEAD
Maximum number of stations in the name table You can reserve space for the working name table, making it either smaller or larger than its default capacity of 2000 station addresses. The maximum will be 8000.	MAXSTNS=*nnnn*
Maximum number of frames for recycled objects The Sniffer Network Analyzer will "forget" network objects that have sent or received fewer than ten frames. To change the number of frames a network object must receive in order to remain on the station list, change the REUSECNT parameter.	REUSECNT
Number of rows or columns in the display screen The analyzer automatically detects the size of the display. These parameters permit you to declare some other size.	ROWS=*nnn* COLS=*nnn*
CGA flicker adjustment Some early CGA monitors will flicker unless access to the screen is confined to retrace. To force the display drivers to wait until retrace, choose WAIT; the analyzer's default is NOWAIT.	WAIT NOWAIT

Figure 11–9. Startup parameters that affect use

Parameter	Values
Expanded memory allocation. The parameters I= and E= do not affect the analyzer itself but rather the expanded memory manager. Within SNSTART.BAT, the line that begins FIXEMM contains uses of I=. These are followed by a reference to **%4**, which passes a use of I= or E= from the .MNU file that invoked SNSTART. The parameter I= or E= is followed by a pair of hexadecimal addresses specifying the beginning and end (inclusive) of a block of extended memory to be included (I) or excluded (E) from the memory made available to the Sniffer analyzer. The starting address must be on a 16K boundary and at least A0000; each is written in 16-byte units, so that (for example) the address C8ff0 appears simply as C8FF (without the trailing 0, or a final H).	I=hhhh-hhhh E=hhhh-hhhh

Figure 11–10. Startup parameters that affect expanded memory

Parameter	Values
Report the Network Interface Card's interrupt level. The parameter IRQ= informs the Sniffer software which interrupt line the adapter card is using.	IRQ=n
Report the Network Interface Card's I/O Addresses. The parameter IOBASE= reports the start of I/O memory. The argument must be written as four hexadecimal digits, without a following H.	IOBASE=hhhh
Report the Network Interface Card's RAM Addresses. The parameter RAMBASE= reports the start of addressable RAM. The argument must be written as four hexadecimal digits, without a following H.	RAMBASE=hhhh
Report the Network Interface Card's DMA Channel. The parameter DMA= reports the number assigned to the adapter card's direct memory access channel. The argument is a one- or two-digit decimal number.	DMA=n
Important: These parameters do not *set* characteristics of the adapter card; they simply report to the Sniffer analyzer a description of the card's characteristics. In most cases, those characteristics are controlled or modified by setting DIP switches or jumpers on the card.	

Figure 11–11. Startup parameters that report the configuration of the adapter card

Symptom and Diagnosis Messages

A

Appendix A. Symptom and Diagnosis Messages

Overview

This appendix lists all the symptom and diagnosis messages generated by the Expert analyzer, and provides a brief description. The messages are grouped by Expert layers; within each layer, they are arranged alphabetically.

This appendix does not provide detailed descriptions of each symptom and diagnosis. When the analyzer generates a symptom or diagnosis you do not understand, pause capture and press F1 **[Explain]** to invoke a context-sensitive Explain message. Explain messages provide detailed descriptions for the analyzer's symptoms and diagnoses.

Symptoms

Application Layer

File retransmission

An entire file, or a subset of a file has been retransmitted. This differs from a transport layer retransmission because the application is purposely retransmitting the file. Each retransmission is counted as a separate symptom.

Loops on same request

The application process on one station sent out the same request even though it has already received the appropriate reply from the destination station. Only requests that are sent within the time specified by **Filter time** are considered "repeated."

Low throughput/Slow file transfer

The rate of throughput during a file transfer was less than the minimum rate specified by the **Local transfer** or **Remote transfer** threshold. Throughput is measured for consecutive bytes within the same file.

Read/write overlap

Read or write requests to a file overlapped each other. For example, if an application wrote bytes 50 through 700, and then wrote bytes 200 through 800, there would be a write overlap because bytes 200-700 were written twice.

Request denied

The number of denied application requests exceeded the **Denied count** threshold. An application request is only counted as denied if it occurs within the time specified by **Filter time**. For more information, see "Filter Time" on page 4–19 and "Denied Count" on page 4–19.

Connection Layer

Ack missing

A REPLY-ACK frame was expected but none was received.

Ack number decreasing

An acknowledgment specifies the segment number of the next octet to be received. The segment number points to the octet's position in the data stream. The amount of data accumulated by the receiver determines what the next octet should be. For example, if octets 1 through 5000 have been received, the receiver specifies the next octet to be 5001. As the transmission progresses, the segment number should increase. A decreasing number causes the sender to send an octet that has already been received. If the analyzer detects this situation, it displays this symptom message.

Ack wrong frame

A REPLY-ACK frame was seen as a response to a REQUEST-DATA frame; REPLY-ACK should only be seen as a response to a REQUEST-DATA-LAST frame.

Bouncing frames

The same frame has appeared twice, but with a decreasing value in the "time-to-live" field. This usually occurs between two routers or gateways, when the same packet is sent between two network stations repeatedly.

Command retransmission

A LAT command frame has been retransmitted. The analyzer tracks the exact number of command frames retransmitted.

Data sent while flow control off

A DECnet data frame was sent while flow control was turned off at the receiving station.

Excessive wait for printer

A user on an AppleTalk connection waited for a response from a printer longer than the **PAP wait** threshold.

Fast retransmission

A retransmission occurred within less than the time specified by the **Fast retrans** threshold.

Refer to "Fast Retransmission" on page 4–23 for more information on this threshold and the related symptoms and diagnoses.

Flow control off for *x* seconds

DECnet flow control was turned off for *x* seconds, which exceeded the threshold specified by **Zero window**.

Idle more than *xx*

No communications were detected between the two end-points of a connection at the transport layer for more than the time specified by the **Idle timer** threshold.

Refer to "Idle Timer" on page 4–23 for more information on this threshold and the related symptoms and diagnoses.

Long ack time

The time that it took the receiver to acknowledge an octet was excessive. The analyzer uses an internal algorithm to determine the threshold. If the threshold is exceeded, it prints the symptom message. The threshold is 3 times the average acknowledgment time plus the **Fast retrans** threshold.

Missing reply

In a request/reply-based protocol (such as Novell PEP), a request was detected, but a corresponding reply was not detected.

Multiple source routing

In a token ring environment, a source-routed packet can be sent from one station to another using multiple paths. This is probably due to incorrect configuration of the token ring bridges.

NFS retransmission

An NFS request has been retransmitted. This is detected by comparing the current RPC transaction identifier with the previous value for this connection.

Packets too close

Two LAT frames are closer than 20ms. The LAT standard is 80ms.

Receive/Continue missing

A RECEIVE-CONTINUE frame was expected as a response to a REQUEST-DATA frame but a different frame was received instead.

Reply retransmission

A LAT reply frame has been retransmitted. The LAT standard states that retransmissions should not occur until at least one second has elapsed from the prior transmission.

Synchronization frame missing

A SYNC frame was expected but none was received.

Transport retransmission

The sequence number is less than or equal to its previous value, indicating that this frame contains data that has already been transmitted.

Window frozen

The TCP window size of the highlighted station has been stuck for longer than the time specified by the **Zero window** threshold.

Window size exceeded

In a windowed protocol (such as TCP or DECnet), the sender sent a segment that contained more data than the receiver's advertised window size.

Wrong reply sequence

The reply sequence number did not match the request sequence number.

Zero window

The TCP window size of the highlighted station has been zero for longer than the duration specified by the threshold **Zero window**.

Network Station Layer

The symptoms and diagnoses at the network layer are concerned with addressing and how traffic is routed from the local network to remote networks.

All paths lost to AppleTalk subnet.

The analyzer has not seen an advertisement for a particular AppleTalk subnet for more than 90 seconds.

AppleTalk corrupt routing table

Some entries in an AppleTalk routing table had illegal or nonsensical values.

AppleTalk network range conflict

An AppleTalk router has advertised overlapping network ranges.

AppleTalk Phase 1 and Phase 2 on same segment

The analyzer has detected AppleTalk Phase 1 and Phase 2 equipment operating on the same local segment. This is sometimes done to reconcile different vintages of equipment, but it causes inefficient use of the network.

AppleTalk suspicious hop count

The analyzer has seen frames from an AppleTalk station, with hop counts differing by more than one from what was expected.

AppleTalk router to nowhere

An AppleTalk router is connected only to the local network.

AppleTalk ZIP Query

The analyzer has detected an AppleTalk ZIP Query packet. Individual ZIP Queries are not a problem — they simply indicate a change in the state of the network. Too many ZIP Queries per minute comprise a ZIP storm, and indicate that a more serious condition exists.

Banyan client unreachable

An ICP exception notification frame indicates that a destination address of a VINES client is not known to a VINES router.

Banyan port unknown

An ICP exception notification frame indicates that a destination port number is not known to a VINES server.

Banyan server down

At least two minutes has elapsed since a Routing Table Update packet or a data frame has been seen from a VINES server.

Banyan server unreachable

An ICP exception notification frame indicates that a destination address of a VINES server is not known to a VINES router.

Destination unreachable

The highlighted station has sent or received ***x*** number of ICMP "destination unreachable" messages.

Duplicate net address

The same network address was mapped to more than one DLC address.

Improper DECnet address

The first four bytes of a DECnet network layer address should always be AA000400. This symptom is generated if a non-conforming address was found in a Long Data or an endnode hello packet.

ICMP error

The highlighted station has received an ICMP message indicating a parameter problem.

Inconsistent server advertisement

Two routers advertise a Novell server with a hop count of one. This hop count value for a Novell SAP means that a router is the server. There may be two network interface cards in the server, or 802.3 and NetWare protocols may be bound to the same card.

Inconsistent subnet mask

The subnet mask specified in an ICMP "address mask reply" message did not match any of the expected subnet masks. The subnet mask could be legitimate, but it is not specified in the STARTUP.ENV file. Use the **Subnet mask** utility in the **Expert config** menu to edit subnet masks.

IP fragment missing

An IP layer fragment on an NFS connection has been lost. This will usually result in an NFS layer retransmission.

IP fragment out of order

An IP layer fragment on an NFS connection was not in sequential order.

ISO error report

One or more ISO error report frames have been seen by the analyzer.

Local router

When the analyzer detects that a router is routing traffic between two local stations, it displays a symptom message. Because the stations are located on the same network, no routing should be necessary.

Many routers to remote

A local station can connect to a remote station through more than one router on the local network.

Multiple routers to local station

The number of routers used to gain access to a local station has equalled or exceeded the **Multiple Routers** threshold.

Network unreachable

The highlighted station has received an ICMP "network unreachable" message.

Port unreachable

The highlighted station has sent an ICMP "port unreachable" message. The message indicates that the station has received a frame sent to the named port, but the port cannot be accessed by the receiving station.

Printer problems

On an AppleTalk network, a printer was not responding, had a paper jam, or was out of paper.

Redirect network/host/frame

The highlighted station has sent an ICMP "redirect host" message. Routers send these messages to inform stations of better routes to desired destinations.

Small hello timer

The rate of DECnet endnode hellos is smaller than the **DEC Hello** threshold. A high rate of DECnet hellos contributes unnecessarily to network overhead.

Source address is broadcast

The source address in a packet is a broadcast address.

Source quench

The highlighted station has received an ICMP "source quench" message. Source quench messages inform stations to reduce their rate of frame transmission.

Time-to-live exceeded

The highlighted station has received an ICMP "Time Exceeded" message. The time-to-live field of the IP layer has reached zero, and therefore the frame has been discarded.

Time-to-live expiring

An IP frame has been detected with a "time-to-live" field equal to 1 or 0, indicating that the frame is about to expire.

Zeros broadcast address

Lists the number of IP frames sent from the highlighted station to an all-zero broadcast address.

DLC Station Layer

Broadcast storm

The rate of broadcast frames sent on the network has exceeded the **Broadcast sy** threshold.

Frame not analyzed

One or more frames were not analyzed by the Expert analyzer. This may happen during heavy network traffic. If the frames are still in the capture buffer, you can overcome this by reanalyzing the data in the capture buffer.

Frame too short

A frame fragment has been detected. The fragment is shorter than the DLC address fields.

LAN overload

The network data rate used a greater percentage of available bandwidth than that specified by the **LAN overload** threshold.

Physical level error

The analyzer has detected a physical level error. If the number of physical errors per second exceeds the **Physical error** threshold, the analyzer will generate a diagnosis. Physical errors include short frames, frames with bad CRCs, and lost frames.

Source DLC address is broadcast

The source DLC address field is a broadcast address.

ZIP storm

The number of AppleTalk ZIP Queries in one minute exceeded the **ZIP storm** threshold.

MAC Layer (Token Ring)

The analyzer captures and reports all MAC level frames on the token ring. Since MAC level frames are essential for troubleshooting token rings, the analyzer reports most MAC frames as symptoms.

Abort error

An "abort delimiter transmitted" MAC condition has been detected.

AC error

The next active upstream neighbor is unable to set the Frame Copied/Address Recognized bits in a frame it has copied.

Bad FC/AR flags

The analyzer has detected an invalid format in the Frame Copied/Address Recognized bits of a frame from the highlighted station.

Burst error

There is a signaling error in the cable. The error is not caused by a station entering or leaving the ring. The Expert analyzer filters out those Burst error frames caused by ring entry and departure.

Duplicate test successful

The Duplicate Address Test MAC frame has been successful (another station on the ring has the same address). When the DLC address of a station trying to enter the ring is the same as the DLC address of a station already in the ring, the station attempting entry is automatically disconnected.

Excessive ring purge

The number of ring purge frames has exceeded the **Rng purge sy** threshold in the **Expert config** menu.

Frame relay buffer depth exceeded

The buffer depth on the router has exceeded a preconfigured threshold. Frames may be lost as a result. If possible, the router should be reconfigured with more buffers.

Internal error

The highlighted station has a recoverable internal error. If the station is reporting multiple internal errors, the station is marginal.

Line error

A "line error" MAC condition has been detected. There was an invalid character in a frame or token, or there was a check error in a frame.

Local node with route designator

Source routing is being used but the source and destination stations are both on the same local ring.

Multiple local ring definitions

Source routing is being used. The routing information in two or more frames is contradictory— that is, two frames have different definitions of the local ring number.

New active monitor

There is a new active monitor on the ring.

Receiver congestion error

The analyzer has detected a Receiver congestion MAC frame. Receiver congestion occurs when a station does not have enough room in its buffer to copy a frame for which it is the destination. If the number of Receiver congestion MAC frames per second exceeds the **RX Congestion** threshold, a diagnosis is generated.

Returned to ring

The highlighted station has reentered the ring, after having left the ring. A new symptom is generated each time the station reenters the ring.

Ring beaconing

The highlighted station has transmitted a Beacon MAC frame in an attempt to bring the ring back into normal operation. This symptom is also a diagnosis.

Station off ring

The highlighted station has left the ring, either purposely or due to a ring problem. A new symptom is generated each time the station leaves the ring.

NOTE: This symptom is not related to the **Stn Removed** diagnosis threshold.

Token error

The token has been lost. This error should only be generated by the active monitor when it recognizes the need to create a new token.

WAN/Synchronous

DISC frame

One or more DISC (disconnect) frames have been received. The HDLC link has been disconnected and must be reestablished before any data transfer can proceed. All previous connections must be renewed.

DLCI bandwidth exceeded

Frame Relay symptom. The measured bandwidth exceeds the requested bandwidth reported in the most recent local management interface (LMI) PVC status frame. The requested bandwidth is the amount guaranteed by the Frame Relay service. It is legal to exceed this amount occasionally, but most Frame Relay services do not guarantee full frame delivery if the value is exceeded.

DLCI keepalive sequence error

Frame Relay symptom. The sequence number in a keepalive LMI frame has been reset to zero. Frames may have been lost immediately prior to this occurrence.

Excessive backward congestion

Frame Relay symptom. The percentage of frames with the Backward Explicit Congestion Notification (BECN) bit set exceeds the **Congestion** % threshold in the **Expert config\Thresholds** menu.

The BECN bit indicates backward congestion on a Frame Relay link. The BECN bit is set by a congested network to notify the user that congestion avoidance procedures should be initiated in the opposite direction of the transmitted frame.

Excessive forward congestion

Frame Relay symptom. The percentage of frames with the Forward Explicit Congestion Notification (FECN) bit set exceeds the **Congestion** % threshold in the **Expert config\Thresholds** menu.

The FECN bit indicates backward congestion on a Frame Relay link. The FECN bit is set by a congested network to notify the user that congestion avoidance procedures should be initiated in the opposite direction of the transmitted frame.

FRMR frame

One or more FRMR (frame reject) frames have been received. FRMR frames indicate an error condition not recoverable by retransmission. Investigate the FRMR frames for more details about the cause of each error.

HDLC retransmission

One or more HDLC numbered information frames have been retransmitted.

Inappropriate SABM

An HDLC SABM (set asynchronous balanced mode) frame has been received, but the Modulo 128 encoding option is currently selected in the **Options** menu of the Sniffer Internetwork Analyzer. This is an inconsistency. You should select the

Modulo 8 encoding option instead. Encoding options are found in the **Options** menu of the analyzer.

Inappropriate SABME

An HDLC SABME (set asynchronous balanced mode extended) frame has been received, but the Modulo 8 encoding option is currently selected in the **Options** menu of the Sniffer Internetwork Analyzer. This is an inconsistency. You should select the Modulo 128 encoding option, instead. Encoding options are found in the **Options** menu of the Sniffer Internetwork Analyzer.

Inappropriate SNRM

An HDLC SNRM (set normal response mode) frame has been received, but the **Frame type** option in the Sniffer Internetwork Analyzer's **Options** menu is not currently set to **SDLC then SNA**. Because the HDLC SNRM frame is usually seen only on an SNA network, you should probably set the **Frame type** option to **SDLC then SNA**.

REJ frame

A REJ (reject) frame has been received. This usually indicates that one or more frames have been lost. If this happens often, check your modem and line for correct operation.

Router buffer overflow

Frame Relay symptom. The buffer depth on the router has exceeded a preconfigured router threshold, possibly causing frames to be lost. Try to reconfigure the router with more buffers.

WAN underload

The Expert analyzer generates the WAN underload symptom when the data rate falls below the percentage of available bandwidth specified by the **WAN underload** threshold in the **Expert config** menu.

WAN congested

The Expert analyzer generates the WAN congested symptom when the data rate exceeds the percentage of available bandwidth specified by the **WAN overload** threshold in the **Expert config** menu.

Diagnoses

Application Layer

Excessive requests denied

This diagnosis indicates that a server has denied an excessive number of application requests relative to the number of successful requests. The related threshold is **Denied request** %.

Refer to "Excessive Requests Denied" on page 5–19 for more information on this diagnosis.

File overlap/retransmission

This diagnosis indicates that the same block of a file is retransmitted between two stations too many times.

When the analyzer counts the number of retransmissions, it also includes the number of file overlaps. Refer to "File Overlap / Retransmission" on page 5–21 for more information on this diagnosis.

Slow file transfer

The analyzer generates the **Slow file transfer** diagnosis when the ratio of slow versus normal file transfers is greater than the **Slow file** % threshold in the Expert config menu. The analyzer uses different thresholds depending on whether frames were routed locally or remotely.

Refer to "Slow File Transfer" on page 5–35 for more information on this diagnosis and the related thresholds.

Slow server

This diagnosis indicates that the analyzer considers the highlighted server slow because of the time it takes for it to respond to application requests.

Refer to "Slow Server" on page 5–36 for more information on this diagnosis and its related thresholds.

Connection Layer

Non-responsive station

The analyzer generates this diagnosis when the number of consecutive identical retransmissions without response on a given connection exceeds the **No responses** threshold in the **Expert config** menu.

Refer to "Non-Responsive Station" on page 5–31 for more information on this diagnosis and related thresholds.

Retransmissions

The analyzer generates this diagnosis when the number of retransmitted frames on a given connection (expressed as a percentage of good transmissions versus retransmissions on the connection) exceeds the **Retransmission percentage** threshold in the Expert config menu.

Refer to "Retransmissions" on page 5–33 for more information on this diagnosis and related thresholds.

Network Station Layer

Duplicate network address

The analyzer generates this diagnosis (and symptom) when two or more DLC stations are associated with the same network address.

Refer to "Duplicate Network Address" on page 5–17 for more information on this diagnosis and related thresholds.

Local router

The analyzer generates this diagnosis when two DLC stations on the same network segment are communicating via two or more routers, rather than directly from one DLC station to the other.

Refer to "Local Router" on page 5–29 for more information on this diagnosis.

Multiple routers to station

The analyzer generates this diagnosis when there are more routers on the local network that can route frames to a remote station than specified by the **Multiple routers** threshold.

Refer to "Multiple Routers to Station" on page 5–30 for more information on this diagnosis and related thresholds.

DLC Station Layer

Broadcast/Multicast storm

The analyzer generates this diagnosis when the number of broadcast/multicast frames per second exceeds the rate specified by **Broadcast dg** in the **Expert config** menu.

Refer to "Broadcast Storm" on page 5–16 for more information on this diagnosis and related thresholds.

LAN overload

The analyzer generates this diagnosis when the rate of network traffic in a given minute is too high. This depends on the settings of the thresholds **LAN overload** and **LAN overload percentage**.

Refer to "LAN Overloaded" on page 5–28 for more information on this diagnosis and the related thresholds.

High rate of physical errors

The analyzer generates this diagnosis when the rate of physical errors per second detected for a particular station exceeds the rate specified by the **Physical errors** threshold.

Refer to "High Rate of Physical Errors" on page 5–23 for more information on this diagnosis and its related threshold.

MAC Layer (Token Ring)

High rate of congestion

The analyzer generates this diagnosis when the rate of MAC receiver congestion errors per second exceeds the rate specified by the **RX Congestion** threshold.

Refer to "High Rate of Congestion" on page 5–22 for more information on this diagnosis and its related threshold.

High rate of line/burst errors

The analyzer generates this diagnosis when the rate of MAC level line plus burst errors for a given station exceeds the **Ring errors** threshold.

Refer to "High Rate of Line or Burst Errors" on page 5–23 for more information on this diagnosis and its related threshold.

High rate of remove from ring requests

The analyzer generates this diagnosis when the rate of MAC level remove from ring requests sent to a given station exceeds the **Stn removed** threshold.

Refer to "High Rate of Remove from Ring Requests" on page 5–24 for more information on this diagnosis and its related threshold.

High rate of ring entries

The analyzer generates this diagnosis when the rate of MAC level ring entries from a given station exceeds the **Ring entries** threshold.

Refer to "High Rate of Ring Entries" on page 5–26 for more information on this diagnosis and its related threshold.

High rate of ring purges

The analyzer generates this diagnosis when the rate of MAC level ring purge frames from a given station exceeds the **Rng purge dg** threshold.

Refer to "High Rate of Ring Purges" on page 5–27 for more information on this diagnosis and its related threshold.

Ring beaconing

The analyzer generates this diagnosis when it detects a MAC level ring beacon frame.

Refer to "Ring Beaconing" on page 5–34 for more information on this diagnosis and its related threshold.

WAN/Synchronous

WAN overloaded

The data rate has exceeded the threshold specified by the **WAN overload** threshold for longer than the duration specified by the **Overload timer** threshold.

Underloaded network

The data rate has fallen below the threshold specified by the **WAN underload** threshold for longer than the duration specified by the **Underload timer** threshold.

Refer to "Underloaded Network" on page 5–37 for more information on this diagnosis and its related thresholds.

Troubleshooting Guide

B

Appendix B. Troubleshooting Guide

This appendix provides solutions to some common problems you may have with the Sniffer analyzer.When you suspect a problem with the analyzer, please look through this checklist before contacting Network General Corporation. Correcting a simple oversight could save you time.

If the suggestions in this chapter do not solve your problem, you can reach Technical Support from 6 a.m. to 6 p.m. Pacific time, weekdays.

Before you call, please note the unit and network interface card serial numbers located on the initialization screen. Also, please have the following information immediately available:

- A record of any error messages exactly, word for word.
- An accurate description of all symptoms of any problem. If you can, describe how to replicate the problem.
- An accurate, up-to-date map of your network that includes LANs as well as interconnecting devices.
- Information and analysis from a trace file, if appropriate.

The following section tells you more about how to reach Network General's Technical Support department.

Network General Corporation Technical Support Department	
Toll-Free Telephone Number	(800) 395-3151
FAX Number	(415) 327-9436
FAX-on-Demand	(800) 764-3329
TDD for the hearing impaired	(415) 327-8723
Internet Address	support@ngc.com
SniffNet BBS (2400 baud)	(415) 327-3875
SniffNet BBS (9600 baud)	(415) 327-4782
CompuServe PC Vendors Forum	GO NETGENERAL

Figure B–1. Accessing the Technical Support department

Communicating with Network General Corporation

This section tells you about the following ways to communicate with Network General's Technical Support department:

- FTP
- CompuServe
- Sniffnet BBS
- Internet email

Using FTP

You can download and upload files using the anonymous FTP service through the Internet. This service is available 24 hours a day, seven days a week.

To access ngcgate via anonymous FTP:

1. From your TCP/IP device, enter the following FTP command:
   `ftp ngcgate.ngc.com`
   or `ftp 161.69.1.1` if you do not have any name resolution.
2. Enter `anonymous` in the Name field and press ENTER.
3. Enter your Internet address in the Password field and press ENTER.

For example, `rogers@ngc.com`. You are now logged into **ngcgate**.

4. Enter the following command to change to the PUB subdirectory:
   `cd pub/updates`
5. Enter `bin` and press ENTER.
   This entry sets the transfer mode to binary and allows proper downloading of files to your computer.
6. Enter the following command to download the desired file:
   `get` ***filename***

Using CompuServe

You can also use CompuServe to download files from Technical Support.

To access CompuServe:

1. Connect your PC to CompuServe via modem.
2. Once logged into CompuServe, enter the following and press ENTER:
   `GO NETGENERAL`
3. Select **LIB14** from the menu.
4. Choose option **4** (Download a file to your computer).
5. Enter the name of the file you want to download (for example, LICENSE.ADD).
6. Select a download protocol from the list presented (use either of the CompuServe-specific protocols).
   You are now ready to begin downloading the file according to your communications software's downloading instructions.

Accessing Sniffnet BBS

If you have a modem, you can log onto Network General's BBS SniffNet to download files from the Technical Support department.

To access the Sniffnet BBS:

1. Configure the computer you are using to call SniffNet with the following settings:
   - Speed: 300-9600 bps
   - Parity: none
   - Stop bits: 1
   - Data bits: 8

2. Dial the SniffNet telephone number: 415-327-3875

   After the modems connect, you will be prompted for a user ID. If you already have one, enter it and your password.

   If you do not have a user ID, enter NEW and press ENTER. Answer all prompted questions. When prompted for a user ID, enter the one you made, enter your new password, and press ENTER.

   Full rights to all areas of the BBS is granted to your new account within 24 hours (working days only). If you need immediate access, please contact Network General's Technical Support at 1-800-395-3151 and ask to be granted immediate full rights.
3. From the Main Menu enter F for the file library and press ENTER.
4. Press **S SHARE** to select the SHARE library.
5. Enter the command D ***filename*** to download the desired file. For example:

   ```
   D LICENSE.ADD
   ```

   A list of protocols is displayed.
6. Select a protocol that your communications software supports and enter a corresponding letter for it.

   Make sure the protocol you selected matches the one selected on the BBS.

   The BBS starts to transmit the file to your computer. You must begin the download procedure on your PC (for example, pressing PGDN in Procomm).

Troubleshooting Checklist

If	There is nothing on the screen	1. Check the power cable and power source. 2. Check the power switch. 3. Make sure the monitor's controls for brightness and contrast are set so the display is visible. 4. If you have a screen-saver program, press any key to redisplay the screen.

If	The Sniffer analyzer program does not start. (It should be present in the main selection menu.)	Make sure there is no diskette in the floppy drive when you start the Sniffer analyzer. (If there is, you may see the message **Non-system disk or disk error.**)

If		
	You cannot capture data from the network	1. Make sure that the capture submenu says **<from Ethernet>** (or **Token Ring**, as the case may be) instead of **<from *filename*>** 2. Check and disable any capture filters.
	...and you are using Ethernet	1. Check the connection from the DB-15, BNC, or TP connector on the analyzer's Ethernet adapter to the Ethernet cable. 2. Check the connection from the Ethernet cable to the transceiver. 3. Check the transceiver, using the instructions provided by its manufacturer. The transceiver may include a light indicating when it is receiving a signal (from the station to which it is connected; in this case the analyzer). Try connecting a different station to the same transceiver or the analyzer to a different transceiver. 4. On an IBM PS2 Model/70, check the **Internal transceiver** (BNC)/**External transceiver** (AUI) options. 5. Restart the analyzer.
	...and you are using token ring	The message "lobe media test failed" probably means that the token ring cable is not attached. Make sure it is plugged into the DB-9 connector for token ring and not the DB-9 connector for video.
	...and you are using ARCNET	1. Check the connection from the BNC connector on the ARCNET adapter to the RG-62 cable from the ARCNET hub unit. 2. Check the network hub unit, using the instructions provided by its manufacturer. The hub may include a light indicating when it is receiving a signal (from the station to which it is connected, in this case the analyzer). Try generating traffic from the analyzer to see if the hub indicator light illuminates. 3. Check the DIP switch for the correct address (that is, other than ARCNET stations on the net).

	...and you are using FDDI	If you are filtering on DLC addresses, check that your address options settings are set appropriately: Show LLC addresses or Show SMT addresses. If the message "Removed from Ring" appears at the top of the screen, the unit may have been disconnected from the ring. Reconnect it.

If	There is no output on the external color monitor	Check that the monitor is powered on and adjusted properly.
	...and you have a Model 30 or 50 Sniffer analyzer	Make sure you select **external color monitor** in the selection menu when you start the Sniffer analyzer.
	... and your Model 20 or 55 Sniffer analyzer has a token ring interface card	Make sure your monitor is attached to the DB-9 connector marked "Video" and not to the DB-9 connector marked "token ring."
	...and you have a Model 70 Sniffer analyzer	The analyzer detects the monitor automatically, if the monitor is already connected when you turn the analyzer on. (On the series 700, there isn't a menu item for an external monitor.) When you attach a monitor: (a) Turn off the analyzer. (b) Connect the monitor to the analyzer's VGA port. (c) Turn the analyzer back on.

If	You do not see any symptoms or diagnoses during Expert capture	1. Check to make sure that the analyzer is accepting frames. If you set the capture filters so that all frames are excluded, the Expert analyzer cannot analyze any frames. 2. Check the settings of **Expert config\Thresholds**. If the thresholds are set too high, the Expert analyzer will not detect symptoms and diagnoses below those thresholds.

If	The diagnosis summary display shows a negative time	The Sniffer Network Analyzer has captured data for more than 20 days. Start a new capture session.

If		
	The % **Analyzed** statistic is very low	The level of network traffic is greater than can be analyzed on a continuous basis. To reduce traffic, you can set a capture filter to analyze frames from a specific server or station only. By using capture filters to reduce the number of frames that need analysis, the % **Analyzed** value will increase. In this way, you can look at each of your servers and routers individually. This will provide you with the Expert symptoms and diagnoses you need to improve network performance and reliability. On a token ring network, you can set the CaptureFrame Slice to 256 bytes. This will make more processor time available for Expert analysis.

If		
	You do not see traffic that you expect	1. Check the station, protocol, and pattern-match capture filters to see whether traffic is being discarded. If the "frames seen" count is larger than the "frames accepted" count, then frames are being discarded.
	...and you are using token ring	1. Check that the ring speed is set correctly on the token ring NIC (16 or 4 Mbits/s). See *Building the Sniffer Network Analyzer* for more information. 2. Check that you are not the only station inserted on the ring. 3. If there are multiple MAUs, check that they are cabled together properly.
	..and you are using a WAN/Synchronous link	1. Check that the **Frame type** is set correctly in the **Options** menu. 2. Is **Frame type** set to **Router/Bridge**? If so, make sure that **Screen format** is set to **Skylines**. Otherwise, you will only see the DTE/DCE counters at the bottom of the screen. See page 3–13 for more information. 3. Check that **Encoding** is set correctly in the **Options** menu.
	...and you see no traffic, but the **lost frames** counter increments	1. Make sure you have no IRQ conflicts between cards.

If	A pattern-match filter or trigger doesn't seem to work	1. Check the protocol and station-address filters; they may be causing the frames of interest to be discarded. 2. Double check the offset; detection of a pattern depends on telling the Sniffer Network Analyzer both what to look for and where to look. 3. Check to make sure the **AND/OR** options are set correctly.
	...and you are looking at frames sent on token ring	Check the offset origin: is it frame-relative (starting with the first frame byte) or data-relative (starting with the first LLC byte)?

If	You get the message "No frames eligible for display"	1. Check the address level display filter, or 2. Check the destination class display filter, or 3. Check the station address display filter, or 4. Check the protocol display filter, or 5. Check the pattern-match display filter. 6. Make sure that the display and capture filters are not mutually exclusive. 7. Use the **Use defaults** option and then redisplay the captured data.

If	You do not see frames that you expect	1. Check the display filters. 2. Check the capture filters, since they may have caused the frames to be discarded

If	Traffic counts during capture show implausible numbers	1. Check that you have selected the appropriate units (frames or kilobytes) in the Capture menu.

If	A "from" or "to" filter isn't working	1. Check the setting of the **Reverse direction** option in the filter menu. 2. Check the settings of other filters involved in capture or display; what you see displayed is what passes through all the filters. 3. Check that an earlier address filter doesn't already accept or discard the frames in question. Recall that filters are examined in sequence.

If	Network utilization seems too low	1. Check the display filters. Remember that only displayed frames are used in the network utilization calculation. Sometimes lower-level protocols that are not displayed carry much of the actual data. 2. Determine whether the frame sizes seem reasonable. The utilization might indeed be correct!

If	You are not seeing symbolic station names	1. Check the **Address level** filters to include addressing at the level you want. 2. Use **Manage names** to examine and add to the names list. 3. Remember to use the **Save names** option to make a permanent change to the name table. 4. On FDDI networks, check **Options** for proper address selection: Show SMT addresses or Show LLC addresses. 5. Make sure the file STARTUP.*xx*D is in the analyzer's current directory (normally, \CAPTURE).

If	HELP information is not available	1. Make sure the file *xx*SNIFF.HLP index file is in the *xx*SNIFF directory. 2. Make sure the various help files are in a subdirectory called HELP within *xx*SNIFF.HLP.

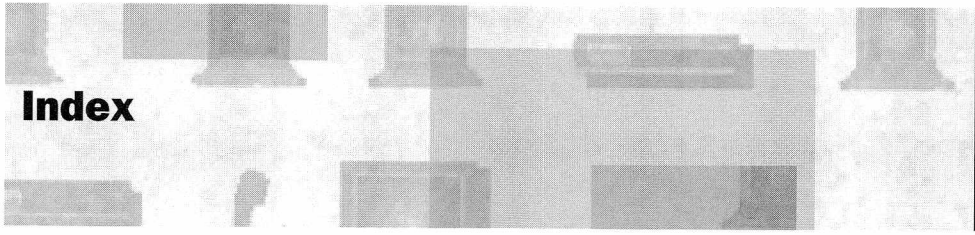
If	You are not getting any print output	1. Check the printer (power, switch settings, and so on). 2. Check that you have selected **LPT1** or **LPT2** (as appropriate) rather than **file** for the printer destination. 3. For serial printers, make sure that the transmit and receive pins are wired correctly. For some printers you may need a **null modem** cable. 4. Check the cable to the printer. For serial printers, make sure you are connecting to the appropriate port. The printer cable needs a DB-9 female connector for the Model 20, 30, 50, and 55. The Model 30 has two serial ports, so be sure you have made the appropriate connections. 5. For serial printers, make sure that you have issued the appropriate MODE command to set the baud rate, word size, parity, and so on.

If	You are not getting all the print output you expect	1. Check the **From frame** and **To frame** options in the **Print** menu. Is **Frame *nnn*** selected instead of **First frame** or **Last frame**? 2. Check the display filters; they affect what is printed. Remember that to print the entire detail report you must select all protocol levels and enable the **All layers** option.

If	You cannot save the capture buffer to a file because your hard disk is full	1. In the **Save data** dialog box, rewrite the path of the target file so that it starts with the drive A:\ or B:\, and write the file to a floppy disk. 2. Move to **Delete files** and delete an unwanted file. Then return to **Save data** and repeat your request.

If	You have found a problem with the Sniffer Network Analyzer software	1. After saving a trace file and the setups to a floppy diskette, try to recreate the problem. Then: • Start the analyzer. • Load the trace file. • Load the setups. • Recreate the problem. If it is a display error, "print" the relevant part of the display to a diskette file. If you can reconstruct the problem in this manner, please send the diskette to the Network General Corporation Technical Support Department. Be sure to include your system serial number and the software version number (displayed in the initialization screen).

If	You have found a problem with the FDDI Sniffer Network Analyzer	1. Check the LED status indicator light on the FDDI adapter board. The LED indicators are: Green: an active connection. Amber: the adapter board is attempting a connection. The adapter board at the other end of the cable is not active, or the cabling is not correct. Red: the board has been enabled and is not attempting a connection.



Index

Index

Symbols

+ sign in detail view 7-50

Numerics

3Com+
    trigger example 6-65
3Com, manufacturer code 11-17
802.2
    IEEE standard 6-43, 6-52, 10-9
802.3
    RI and IEEE standard 10-10

A

A flag 7-41
Abort error
    MAC symptom A-11
Abort flag 7-41
Absolute time display option 7-36, 7-42
absolute utilization
    field in statistics windows 5-68, 5-69
AC error
    MAC symptom A-12
ACC
    and the Internetwork analyzer
        Internetwork Analyzer
            and ACC bridge/routers 3-14
ACC, manufacturer code 11-17
Acer, manufacturer code 11-17
Ack missing
    symptom A-4
Ack number decreasing
    symptom A-4
Ack wrong frame
    symptom A-4
active
    FDDI station 3-17
    panel 7-31
    token ring monitor 1-5
    vs. completed calls 6-27
active stations
    field in Global Symptoms detail window 5-60
active time
    field in Global Symptoms detail window 5-60
address
    6-byte DLC 7-66
    additional name table 11-13
    bits in memory vs. bits on wire 7-66, 11-17
    Broadcast option 6-38
    count 6-20
    display filter 7-11
    DLC destination 6-39
    DLC vs. higher level filter 7-9
    FDDI 3-18, 7-32
    filter
        any station 6-40
        fewer than four matches 6-40
        include/exclude others 6-40
        order of checking 6-40
    format 7-46, 7-47
    generic 6-38
    higher level 8-8
    higher level display format 7-46
    IEEE
        manufacturer's codes 7-66
        standard for bit order 7-67
    IEEE standard for bit order 11-17
    joint effect of several filters 6-40
    logical call 6-26
    match capture filter 6-9
    name assignment 7-14
    remote 6-26, 6-27
    Specific option 6-38
    specific vs. generic 6-38, 7-10
    station 10-5
    symbolic name 8-3
    type, in name table 8-4, 11-15

width of field 4-37, 7-34
address level
display filter 7-5, 7-6, 7-9
effect on name table 11-15
address recognized, token ring frame 7-71
addrtype, name table field 11-14
adjusting scales in skyline views 6-30
Agilis, manufacturer code 11-17
Alantec, manufacturer code 11-17
All layers display option 7-33, 7-36
effect on detail view 7-45
Altos, manufacturer code 11-17
Ameristar Technology, manufacturer code 11-17
analyzer present, token ring broadcast 1-5
AND, combining patterns 6-47
Apollo, manufacturer code 11-17
appl ID
counter 5-55
Apple, manufacturer code 11-17
AppleTalk 4-24, 4-27, A-7, A-11
format of DDP address 7-47
application layer
available Expert triggers 6-72
detail window 5-55
Expert thresholds 4-18
list of diagnoses A-16
list of symptoms A-3
OSI vs. Expert layer 4-5
Statistics window 5-63
application layer, OSI model 7-30
application requests
field in statistics window 5-63
applying current setup options 8-23
AR, network abbreviation in file name 11-5
ARCNET
address format 6-40
display during capture 6-21
display options 7-35
matrix view 6-3, 6-21
octal format 6-40
probe 6-21
Ardent, manufacturer code 11-17
arithmetic fields, byte order 11-21
arrival time field in trace file 11-20
arrow flag 7-41
ASCII
interpretation in hex view 7-51
parity option 7-51
ASN.1, ISO protocol interpretation 7-68
associated DLC addresses
field in statistics window 5-68
associated network stations
field in statistics window 5-70
asterisk
meaning in Expert displays 5-11
AT&T, manufacturer code 11-17
Audible 6-16
Audible clicks option 3-5, 6-16
AUTOEXEC.BAT file 11-6
average frame length
field in statistics window 5-66
average load %
field in Global Symptoms detail window 5-60

B

Bad CRC frames capture filter 6-34, 6-35, 6-58
Bad CRC frames display filter 7-6, 7-17
Bad FC/AR flags
MAC symptom A-12
bandwidth
field in Global Stats window 5-75
percentage utilization 5-74
Banyan Vines
and the Internetwork analyzer 3-14
bar graph 6-16
linear vs. log scale 6-17
units 6-15
baseline
network 4-13
batch file
AUTOEXEC.BAT 11-6

BBN, manufacturer code 11-17
beacon, token ring 3-12
beam splitter
    FDDI option 3-18
BICC, manufacturer code 11-17
binary
    field interpretation 7-67
bit reversal
    transmission of DLC address 11-17
bit-level interpretation 7-67
Bouncing frames
    symptom A-4
Bridge, manufacturer code 11-17
Broadcast
    filter 7-10
    option 6-38
Broadcast dg
    Expert threshold 4-27
Broadcast storm
    Diagnosis Detail display 5-16
    symptom A-11
Broadcast sy
    Expert threshold 4-27
broadcasts
    field in Global Symptoms detail window 5-60
broken connection
    how analyzer calculates 5-31
Burst error
    MAC symptom A-12
byte order, numeric field in trace file 11-21
bytes
    counter in summary windows 5-41
    display of counts 6-18, 6-28
    display option 7-43
    units 6-15
    written field in trace file 11-20
bytes transferred
    field in statistics window 5-63

C

C flag 7-41
cable test
    and the Notebook Sniffer Analyzer 6-4
    automatic 6-5
    Ethernet 1-5
    fault diagnosis 6-6
    in Options menu 3-7
    jittering display 6-6
    menu option 6-4
capture
    automatic cable test 6-5
    bar graph displayed 6-16
    capture mode 6-10
    clearing screen 6-20
    counters in skyline view 6-28
    counters in tabular view 6-16, 6-18
    customizing 4-35
    discarding previous buffer 6-75
    display active/all calls 6-27
    displaying active/all calls 6-27
    DLC address in filter 6-39
    higher level protocols 6-46
    Highspeed mode 6-32
    highspeed mode 6-32
    individual counts 6-20
    limitations of capturing from a file 6-12
    live network vs. playback from file 6-11
    overview of process 6-8
    pair counts 6-19
    pausing 6-27, 6-74
    preparations for 6-8
    resuming paused capture 6-28
    saving capture filters 6-36
    selecting mode 1-10, 2-6
    source of frames 6-9
    starting 6-74, 7-52
    stopping 6-28, 6-61, 6-74
    time required for filters 6-35
    vs. display 1-4
capture buffer
    discarding captured frames 6-75
    file format 11-18
    loading 8-16
    printing 7-60
    printing or importing 11-18

reported size 6-7
role in display 7-4
save to file 6-75, 8-11
searching for frames 7-55
CAPTURE directory 11-8, 11-12, 11-13
capture filters 6-9
Bad CRC frames 6-34
Collision frames 6-34
Destination class 6-34
disabling temporarily 6-36
effect on name table 6-37
effects on Global Statistics 5-76
example 6-55
From DCE 6-35
From DTE 6-35
Good frames 6-34
Known stations only 6-34
overview 6-33
Pattern match 6-34, 6-46
Protocol 6-34
RNR frames 6-35
RR frames 6-35
Short frames 6-34
Station address 6-34
Unknown stations only 6-34
Cayman, manufacturer code 11-17
CDC, manufacturer code 11-17
changing directories 11-10
character
interpretation of ASCII or EBCDIC 7-51
CIMlinc, manufacturer code 11-17
Cisco
and the Internetwork Analyzer 3-14
manufacturer code 11-17
claim frame capture filter 6-34
Classic mode option 6-9, 6-10
Clear all names option 8-11
clearing
counters during capture 6-20
name table 8-11
screen during capture 6-21, 6-27
CMC, manufacturer code 11-17
collision
effect on cable test 6-6
Collision flag 7-41
collision frames 10-6
Collision frames capture filter 6-34, 6-58
Collision frames display filter 7-6, 7-17
color in display 7-29
combining patterns 6-47, 6-49
ComDesign, manufacturer code 11-17
Command retransmission
LAT symptom A-4
comment line in name table 11-15
composition of traffic by protocol family
fields in Global Stats window 5-73
CONFIG directory 11-7
configuration
Expert analyzer 4-7
STARTUP.xxV 4-7
subnet masks 4-7
Congestion percentage
as calculated for Frame Relay 4-32
as calculated for HDLC 4-32
Expert threshold 4-32
conn
field in summary windows 5-41
connection layer
available Expert triggers 6-72
detail window
DLC Station layer
detail window 5-55
Expert thresholds 4-22
list of diagnoses A-17
list of symptoms A-4
OSI vs. Expert layer 4-5
Statistics window 5-65
connections to net stations
field in statistics window 5-68
conventions
in Sniffer manuals xxxv
conversion utility
LM2000 and Internetwork Analyzer 8-13
timestamps 8-16

copy and paste
pattern and offset 6-55, 7-47
counters
appl ID 5-55
associated DLC addresses 5-68
connections to net stations 5-68
diagnosis 2-7
duration 5-11
first time 5-11
in Detail windows 5-54
in the Summary window 5-42
inter-frame time 5-64
transfers data for 5-70
CRC flag 7-41
creating
a directory 11-9
creating bad CRC frames 7-55
CSV data 3-23, 8-18, 11-8
CSV format 7-63, 11-18
comma separated values 7-62
comparison of file and screen output 7-65
Cumulative bytes display option 7-43
cursor keys
next line or frame 7-52
cut and paste
pattern and offset 7-47

D

data files
contents 11-19
format 11-8
loading 6-75
name 11-8
Data General, manufacturer code 11-17
data link layer
OSI vs. Expert layer 4-5
data relative option 3-6, 6-52
Data sent while flow control off
DECnet symptom A-5
date format in trace file 11-19
days since start field in trace file 11-20
DCA, manufacturer code 11-17
DCE
as relates to Underload calculation 4-31
DDP, address format 7-47
DEC hello
Expert threshold 4-24
to measure duplicate addresses 4-25
DEC keep alive
Expert threshold 4-23
DEC, manufacturer code 11-17
DECnet
address format 7-47
learning names
4-37
DECnet, manufacturer code 11-17
defaults
resetting for thresholds 4-14
restoring 3-7, 11-13
subnet masks 4-8
defective frames
display filters 7-16
Defective frames capture filters 6-9
defective frames trigger 6-9
deleting
data files 8-18
names from the name table 8-11
Delimited format option 7-62, 11-18
Delta time display option 7-36, 7-43
Denied count
Expert threshold 4-19
Denied req%
Expert threshold 4-20
destination address
generated frame 10-5
generic 6-38
Destination class capture filter 6-9, 6-34, 6-37, 6-38
Destination class display filter 7-5, 7-10
Destination unreachable
symptom A-7
Detail Diagnosis windows 5-14
detail view 7-27, 7-44

+ sign 7-50
continuation to following frame 7-50
format of higher level address 7-46
printing 7-44
protocol layers 7-45
synchronization with hex view 7-30, 7-48
synchronization with summary view 7-45, 7-67
treatment of "address recognized" bits 7-71
Detail window
displaying 5-52
for subnet pairs 5-56
Global Symptoms 5-58
information in 2-17, 5-54
overview 5-6
symptom and network object 5-52
DG, manufacturer code 11-17
diagnoses
column in Expert Overview 5-8
diagnosis
and the Expert analyzer 2-4
Broadcast storm 5-16
counter 2-7
defined 2-4
Detail windows 5-14
displays in the Expert window 5-10
Duplicate Network Address 5-17
Excessive Repeated Requests 5-18
Excessive Requests Denied 5-19
File Overlap/Retransmission 5-21
getting more information 2-8
High Rate of Congestion 5-22
High Rate of Line/Burst Errors 5-23
High Rate of Physical Errors 5-23
High Rate of Remove from Ring Requests 5-24
High Rate of Ring Entries 5-26
High Rate of Ring Purges 5-27
LAN Overloaded 5-28
listed at application layer A-16
listed at connection layer A-17
listed at DLC Station layer A-18
listed at MAC layer A-18
listed at network station layer A-17
listed for WAN/Synchronous A-19
Local router 5-29
Multiple Routers to Station 5-30
Non-responsive station 5-31
Overview display 2-8
restoring to display 5-12
Retransmissions 5-33
Ring Beaconing 5-34
setting thresholds for 4-13
Slow File Transfer 5-35
Slow Server 5-36
Summary display 5-10
temporarily removing 5-12
Underloaded Network 5-37
using as a filter 7-17
using as trigger event 6-69
directory
CAPTURE 11-8, 11-13
changing 11-10
CONFIG 11-7
create new 11-9
DOS 11-6
organization 11-6
root 11-6
SNIFF 11-7, 11-8
TOOLS 11-7
DISC frame
WAN/Synchronous symptom A-13
discarding captured frames 6-75
disconnect
token ring 3-12
Disk snapshot option 6-9, 6-63, 6-66
display
active view 7-31
active/all calls during capture 6-27
automatic scan for station addresses 8-5, 8-6
capture buffer 6-75
detail view 7-27, 7-45
enlarging views 7-32
help menu 6-27
in the Expert window 5-6
LAN display filters 7-5
manufacturer's code in addresses 7-34
name width 7-35
network volume 6-28
options 7-59

overview of views 7-27
role of capture buffer 7-4
scrolling within views 7-30
search for pattern 7-59
search for text 7-59
setting filters 7-7
spanned frames 7-49
summary view 7-27, 7-33
synchronization between views 7-30
types available in Expert window 2-7
use of color 7-29
vs. capture 1-4
WAN/synchronous display filters 7-6
width of name field 4-37, 7-34
display filters 7-5
address level 7-9
defective frames 7-16
destination class 7-10
for the Expert analyzer 7-17
pattern match 7-15
selected frames 7-16
station address 7-11
symptom frames 7-24
Displaying
Help menu by pressing F1 1-14
DLC
address 7-9
address format 7-47, 11-15
addresses display option 7-36, 7-38
capture filter 6-39
header AC and FC bytes 10-14
protocol, 6-byte address standards 7-66
SAP, protocol filter 6-43
DLC addr
field in detail windows 5-55
DLC addresses display option 7-38
DLC name
field in detail windows 5-55
DLC Station Address
field in summary window 5-42
DLC Station layer
available Expert triggers 6-72
Expert thresholds 4-25
list of diagnoses A-18
list of symptoms A-11
OSI vs. Expert layer 4-5
Statistics window 5-68
DLCI 6-25
DLCI bandwidth exceeded
WAN/Synchronous symptom A-14
DLCI keepalive sequence error
WAN/Synchronous symptom A-14
don't match 6-50
DOS
directory 11-6
path 11-6
Dove, manufacturer code 11-17
DRP
address format 7-47
DSAP, example 10-15
DTE
as relates to Underload calculation 4-31
DTE/DCE counters scale 6-17
Duplicate Network Address
Diagnosis Detail display 5-17
symptom A-8
Duplicate test successful
token ring symptom A-12
Duplicate%
thresholds 4-24
duration
counter in summary windows 5-11
difference from elapsed time counter 5-75
field in Global Stats window 5-75
Dynamic mode option 7-51

E

E flag 7-41
EBCDIC, interpetation in hex view 7-51
Edit names option 8-6
Edited flag 7-41
editing
frames in hex view 7-53
name table 8-6

startup parameters 11-22
either offset 6-49
with OR 6-50
encoding schemes 3-14
Encore, manufacturer code 11-17
end of file, trace file record 11-19
error frame capture filter 6-34
error status field in trace file 11-20
Ethernet
address format 7-47
available capture filters 6-34
cable test 1-5
data field within frame 10-10
defective frames capture filters 6-58
defective frames display filters 7-16
display filters 7-6
DLC address 7-33
flags 7-41
generic address format 6-39
Highspeed mode option 6-9, 6-10, 6-32
internal trigger 6-62
minimum frame size 10-6
network code in trace file 11-20
system options 3-4
trigger example 6-65
valid fame size 10-6
Ethernet-II
collision frames 6-59
Collision frames capture filter 6-34, 6-58
Ethertype
example 7-45
protocol filter 6-43
Excelan, manufacturer code 11-17
Excessive Backward Congestion
as calculated for Frame Relay nets 4-32
WAN/Synchronous symptom A-14
Excessive Forward Congestion
as calculated for Frame Relay nets 4-32
WAN/Synchronous symptom A-14
Excessive Repeated Requests
Diagnosis Detail display 5-18
Excessive Requests Denied
Diagnosis Detail display 5-19
Excessive ring purge
MAC symptom A-12
Exclude others option, Station address filter 6-40
Expert analyzer
and diagnoses 2-4
and learning names 4-37
and network objects 2-3
and symptoms 2-4
application layer 4-5
configuration 4-7
configuring subnet masks 4-9
configuring trustee names 4-12
connection layer 4-5
description of capture 2-3
Detail windows 2-17, 5-6
Diagnosis Summary display 5-10
display filters 7-17
DLC Station layer 4-5
effects of changing thresholds 4-32
excluding trustee names 4-12
Expert layers 4-4
Expert Overview window 5-5
Expert window 2-7
Freeze/Reuse allocation option 4-35
function keys 5-80
Global Statistics view 5-6
layers 2-7
main menu 1-9
navigating displays 5-6
network object filter 7-17
network station layer 4-5
overview of displays 2-16
protocols available for analysis 2-20
setting subnet masks 4-7
setting thresholds 4-13
starting in Expert mode 2-3
Statistics windows 2-18, 5-6, 5-60
Summary windows 2-16, 5-5
symptom and network object displays 5-38
symptom detail windows 5-52
terminology 2-3
Expert data 3-23, 8-18, 11-8
Expert Overview

and navigating through the analyzer 5-8
as home base for analysis 5-3
diagnoses column 5-8
explained 5-8
objects column 5-8
symptoms column 5-8
Expert threshold 4-28
Expert window
defined 2-7
displaying analysis results in 5-3
function keys 5-80
navigating displays 5-6
overview of displays 2-16
Explain
defined 2-10
F1 2-10
sample screen 2-10
to display a message 2-10
user 2-12
using to investigate network problems 5-12
vs. help screens 2-10
explain
changing language of 3-4
external trigger 6-9, 6-62

F

F1
Explain 2-10, 5-12, 5-80
help 5-80
F1, displaying Help menu 1-14
F10
start capture 7-52
stop capture 5-80, 6-74
stop/new capture 5-81
F2
displaying Global Statistics 5-72
filter&disply 5-80, 7-17
set mark 7-51
to view Global Statistics 5-80
F3
display 5-81
display capture buffer 7-52
toggle between Expert and Classic windows 5-81
F4
changing formats of Summary window 5-43
view DLC Stn/Protocol/Symptom 5-80
zoom 7-52
F5
menus 5-81, 7-52
return to main menu 7-52
F6
capture options 5-81
display options 7-52, 7-59
scale down 6-31
F7
go to previous frame 7-52
higher layer 5-81
remove diag 5-12, 5-80, 5-81
view earlier 6-31
F8
go to next frame 7-52
lower layer 5-81
restore diags 5-12, 5-80, 5-81
view later 6-31
F9
pause 5-80
pause/resume capture 5-81, 6-31, 6-74
Fast retrans
Expert threshold 4-23
Fast retransmission
symptom A-5
fault
cable 6-4
FDDI
active station 1-6, 3-17
address format 7-47
addressing 3-18
beam splitter 3-18
error frame capture filter 6-34
options 3-17
scrolling large capture buffer 7-31
Show LLC addresses option 3-18, 7-32
Show SMT addresses option 3-18, 7-32
void frame capture filter 6-34
void/claim frame capture filter 6-34
field

delimiter in CSV format 7-62
printed report 7-60
width of name 4-37, 7-34
file
capture from playback 6-11, 6-75
captured frames 6-75
filename limitations 11-9
format of captured frames 11-18
name table format 11-10, 11-13
playback of capture 6-11
printer output 7-63, 11-18
STARTUP.xxV 4-7
file format
capture buffer 11-18
CSV format 11-18
output files 11-18
File Overlap/Retransmission
Diagnosis Detail display 5-21
File retransmission
symptom A-3
files
menu item (whole chapter) 8-11
filter
time required during capture 6-35
Filter time
Expert threshold 4-19
filters
Expert display filters 7-17
first time
counter in summary windows 5-11
flags
defective frames 6-59
Flags option 7-40
Flip DLC address option 7-32
Flow control off for x seconds
DECnet symptom A-5
force protocol
disabling 9-13
form feed, printed report 7-65
format
file of captured frames 11-18
higher level address 7-46
name table 11-13, 11-14
printed report 7-60, 11-18
version record in trace file 11-19
fragmentation protocol, OSI model 7-30
frame
quantity to generate 10-7
frame copied, token ring 7-71
frame counts during capture 6-15
Frame editing option 7-53
frame error status field in trace file 11-20
Frame not analyzed
symptom A-11
frame record field in trace file 11-19
frame relative option 3-6, 6-52
Frame Relay
about the global protocol family counter 5-73
and the calculation of Congestion percentage 4-32
Frame relay buffer depth exceeded
symptom A-12
Frame relay protocol 3-13, 6-23
frame size
effects on Global Statistics 5-76
Frame size option 6-9
Frame too short
symptom A-11
Frame type option 3-13, 6-24
frames
captured and saved to file 6-75
counters 6-18
discarded at new capture 6-75
field in subnet detail window 5-57
field in subnet summary windows 5-49
Freeze/Reuse allocation option 4-36
FRMR frame
WAN/Synchronous symptom A-14
From DCE
Global Statistics field 5-74
From DCE capture filter 6-35, 6-60
From DTE
Global Statistics field 5-74

From DTE capture filter 6-35, 6-60
function keys
display options 7-52
during capture, LAN tabular views 6-22
during capture, skyline view 6-31
during capture, WAN/Synchronous 6-27
during capture, WAN/synchronous 6-22
during Classic display 7-51
in the Expert window 5-80
menus 7-52
new capture 7-52
next frame 7-52
pause or resume capture 6-74
previous frame 7-52
set mark 7-51
stop or start capture 6-74
while capture is paused 6-74
zoom 7-52

G

generate traffic 1-5
generated frame
destination address 10-5
interval 10-6
number to be generated 10-7
RI field 10-9
size 10-5
structure 10-8
Global Statistics
display using F2 5-80
effects of capture filters on 5-76
effects of Frame Size option 5-76
fields composing 5-73
overview 5-6
overview of window 5-72
percent analyzed field 5-76
percentage bandwidth utilization fields 5-74
run information fields 5-74
start run field 5-75
to display the window 5-72
Global Symptoms
Detail window 5-58
summary window defined 5-50
glue layer 7-30
Good frames capture filter 6-34, 6-58
Good frames display filter 7-6, 7-16, 7-17
Gould, manufacturer code 11-17

H

HDLC
and the calculation of Congestion percentage 4-32
HDLC protocol 3-13, 6-23, 6-25, 6-26
HDLC retransmission
WAN/Synchronous symptom A-14
header
effect of truncating stored frame 6-10
trace file 11-19
heading, printed output 7-65
help
changing language of 3-4
F1 6-74
menu 6-27
vs. Expert explain 2-10
hex view 7-47
defining interpretation of characters 7-51
synchronization with detail view 7-30, 7-48, 7-67
hexadecimal
data for pattern match 6-51
High Rate of Congestion
Diagnosis Detail display 5-22
High Rate of Line/Burst Errors
Diagnosis Detail display 5-23
High Rate of Physical Errors
Diagnosis Detail display 5-23
High Rate of Remove from Ring Requests
Diagnosis Detail display 5-24
High Rate of Ring Entries
Diagnosis Detail display 5-26
High Rate of Ring Purges
Diagnosis Detail display 5-27
higher level protocol
address formats 7-46
frames that span several DLC frames 7-50

interpretation 7-67
highlight
menu selection 1-13
high-order-bit first
transmission order 7-66, 11-17
Highspeed mode option 6-9, 6-32
hop count
field in subnet detail window 5-57
hops
field in statistics window 5-63
field in subnet summary window 5-49
H-P Intelligent Networks Oper, manufacturer code 11-17
H-P, manufacturer code 11-17

I

IBM
routers and the Internetwork Analyzer 3-14
IBM protocol suite, trigger example 6-65
ICMP error
symptom A-8
icons
in Sniffer manuals xxxvi
Idle more than xx
symptom A-5
Idle timer
Expert threshold 4-23
IDs of manufacturers
table of names and codes 11-17
IEEE
802.2 6-43, 6-52, 10-9
802.3 and RI 10-10
standard for transmission of DLC address 7-67
import name table for station addresses 11-13
Improper DECnet address
symptom A-8
Inappropriate SABM
WAN/Synchronous symptom A-14
Inappropriate SABME
WAN/Synchronous symptom A-15
Inappropriate SNRM
WAN/Synchronous symptom A-15
Include others option, Station address filter 6-40
Inconsistent server advertisement
symptom A-8
Inconsistent subnet mask
symptom A-8
individual counts during capture 6-20
Info frames capture filter 6-35
initialization
name table 11-13
STARTUP file 8-23
Intel, manufacturer code 11-17
inter-frame time
field in statistics window 5-64
how calculated 5-65
Intergraph, manufacturer code 11-17
Interlan, manufacturer code 11-17
Internal error
MAC symptom A-12
internal trigger 6-62
Internetwork Analyzer
and Banyan Vines bridge/routers 3-14
and Cisco routers 3-14
and IBM routers 3-14
and Microcom bridge/routers 3-14
and Proteon routers 3-14
and Ungermann-Bass bridge/routers 3-14
and Vitalink routers 3-14
and Wellfleet routers 3-14
Expert thresholds 4-30
frame counts during capture 6-23
Frame type options 3-13
line interface options 3-15
list of diagnoses A-19
list of symptoms A-13
LM2000 conversion utility 8-13
Router/Bridge frame type 3-13
RS232 line interface 3-15
RS422 line interface 3-15
RS423 line interface 3-15
T1 interface via T-POD 3-15
V.10 line interface 3-15
V.11 line interface 3-15

V.35 line interface 3-15
Interpret RI option 3-5
interval
traffic generator 10-6
Invert (data bits) option 3-15
IP
address format 7-46, 7-47, 11-15
address level 7-9
example 7-45
protocol filter 6-45
protocol number for TCP 6-56
setting IP addresses 4-7
IP fragment missing
symptom A-8
IP fragment out of order
symptom A-9
IPX
address format 7-47
ISO
frames that span several DLC frames 7-50
interpretation of ASN.1 7-68
spanned frames 6-11

J

jumping
to marked frame 7-60
to trigger frame 7-60

K

kilobytes
counts during capture 6-16
display of counts 6-28
units 6-15
Kinetix, manufacturer code 11-17
Known stations only capture filter 6-9, 6-34, 6-37, 6-38

L

L flag 7-41
LAN
capture display options 6-13
display filters 7-5
function keys during capture 6-22
network usage during capture 6-16
LAN Manager
token ring functional address 1-5
LAN overload
Expert threshold 4-26
symptom A-11
LAN overload%
Expert threshold 4-26
LAN Overloaded
diagnosis detail display 5-28
language
in Options menu 3-4
last symptom
field in summary windows 5-42
layers
on the Expert analyzer 2-7
on the Expert analyzerlayers 4-4
LCN 6-26
length field in trace file header 11-19
Line error
MAC symptom A-12
line interface
options for Internetwork Analyzer 3-15
linear scale, bar graphs 6-17
lines per page 7-66
link layer, OSI model 7-30
LM2000
Internetwork Analyzer conversion utility 8-13
loading
capture buffer with data file 8-16
data files 6-75, 8-17
setup files 8-23, 11-12
Local node with route designator
MAC symptom A-12
Local router
Diagnosis Detail display 5-29
symptom A-9
Local xfer
Exper threshold 4-21
LocalTalk

address format 6-40, 7-47
display during capture 6-21
matrix view 6-3
network code in trace file 11-20
logarithmic scale, bar graph 6-17
logic, combination of several patterns 6-47
logical calls 6-26
Long ack time
symptom A-5
Look for names option 6-37, 8-6, 8-10
Loop%
Expert threshold 4-20
Loops on same request
symptom A-3
lost frame
effect of capture filter 6-35
effect of truncation 6-10
highspeed capture 6-32
Lost frame flag 7-41
lost frames
counter 6-35
counter for Token Ring-III 6-23
Low throughput/Slow file transfer
symptom A-3
low-order-bit first
transmission order 7-66, 11-17
LT, network abbreviation in file name 11-5

M

MAC layer
available Expert triggers 6-72
Expert thresholds 4-28
list of diagnoses A-18
list of symptoms A-11
main menu
Expert analyzer 1-9
main selection menu 1-8
make directory 11-9
Manage names option 8-4
manuals
Sniffer Network Analyzer xxxviii
manufacturer ID
file format 11-16
table of names and codes 11-17
Many routers to remote
symptom A-9
Mark flag 7-40
match
enable/disable 6-40
fewer than four 6-40
order of checking 6-40
matrix view, ARCNET 6-21
max load %
field in Global Symptoms detail window 5-60
memory
Freeze/Reuse allocation option 4-35
report of allocation 6-7
representation of transmitted address 7-66
menu
generated by .MNU files 11-7, 11-8
panels 1-13
Metaphor, manufacturer code 11-17
Microcom
and Encoding to Modulo-128 3-14
and the Internetwork analyzer 3-14
Min appl req
threshold 4-18
minimum frame size 10-6
MIPS, manufacturer code 11-17
Missing reply
symptom A-5
MNU file extension 11-22
MNU, file extension for menu file 11-7, 11-8
mode
beam splitter 3-18
Model 70
setting token ring speed 3-10
setting transceiver option 3-8
Modulo 128 3-15
Modulo 8 3-15
mouse usage 1-14
Moving within Help menu 1-14

Mult routers
Expert threshold 4-24
Multiple local ring definitions
MAC symptom A-13
Multiple routers to local station
Diagnosis Detail display 5-30
symptom A-9
Multiple source routing
token ring symptom A-5

N

name
common Novell names to exclude 4-12
excluding Novell trustee names 4-12
Expert and remote stations 5-56
field width in display 4-37, 7-34, 7-35
tricks for learning w/Expert 4-38
using Expert to learn 4-37
name files
creating 11-14
format 11-14
type of address 11-15
name table
adding addresses 7-14
alphabetization of names 11-16
automatic address scan 8-5, 8-6
clearing 8-11
comment line 11-15
contents 8-4
create new 11-14
default type 11-16
editing 8-6, 8-7
effect of capture filters 6-37
explicit and implicit declarations of address type 11-15
file format 11-12, 11-13, 11-14
increasing maximum stations 11-22
looking for higher level addresses 8-10
maximum number of addresses 8-3
new station 6-43, 7-13
overview 8-3
protocol layers 8-8
resolving names with external files 8-9
saving 8-8, 8-10, 8-11
supplementing with external file 11-13
unknown station 6-38
using Expert to learn 4-37
Name width display option 4-37, 7-34
NBI, manufacturer code 11-17
Nestar, manufacturer code 11-17
net addr
field in detail windows 5-55
net name
field in detail windows 5-55
net station address
field in summary window 5-42
network
baseline 4-13
role of Sniffer analyzer 1-5
Network Computing Devices, manufacturer code 11-17
network field in trace file 11-19
Network General, manufacturer code 11-17
network layer
OSI vs. Expert layers 4-5
network layer, OSI model 7-30
network object
and changed thresholds 4-32
and the Expert analyzer 2-3
and the Freeze/Reuse allocation option 4-35
defined 2-3
Detail windows 5-52
Freeze/Reuse allocation option 4-35
getting more information 2-16
how Expert reuses 4-36
overview of related displays 2-16
related displays in the Expert window 5-38
Statistics window 5-60
Summary displays 5-38
Network object display filter 7-17
displaying 7-22
limitations 7-22
removing 7-24
setting 7-18
network station layer
available Expert triggers 6-72

detail window 5-55
Expert thresholds 4-24
list of diagnoses A-17
list of symptoms A-7
OSI vs. Expert layer 4-5
Statistics window 5-67
Network Systems Corp, manufacturer code 11-17
Network Underload
symptom 4-31
Network unreachable
ICMP symptom A-9
Network utilization display option 7-43
network volume 6-28
New active monitor
MAC symptom A-13
new capture
F10 7-52
new directory 11-9
new station
adding to name table 7-13
edit name table 6-43, 8-8
next frame, function key 7-52
NeXT, manufacturer code 11-17
NFS retransmission
symptom A-6
No responses
Expert threshold 4-22
No signal-remove token ring option 3-11
Non-responsive station
Diagnosis Detail display 5-31
NOT, combining patterns 6-47
Novell
learning names 4-37
setting trustee names 4-12
system code 6-45
Novell, manufacturer code 11-17
NRZ 3-15
NRZI 3-15
numeric field, byte order 11-21
NW utilization display option 7-36

O

O flag 7-41
objects
column in Expert Overview 5-8
offset
copy and paste procedure 6-55
either 6-49
pattern 6-49, 7-47, 7-59
on-line help, F1 6-74
options
beam splitter 3-18
cable test 3-7
Freeze/Reuse allocation 4-35
menu item (whole chapter) 3-3
OR 6-47
with either offset 6-50
order
bits within byte 7-66, 11-17
bytes in numeric field of trace file 11-21
organization, directories 11-6
OSI model
vs. Expert layers 4-4
Others option, Station address filter 6-40
output
printer page titles 7-65
to file 7-63
to printer 7-63
Overcongested WAN
as calculated for HDLC 4-32
Overload timer
Expert threshold 4-31
Overrun flag 7-41
Overwrite files option 6-66

P

P1
X.400 protocol example 7-69
packet data length
field in statistics window 5-64
Packets too close
LAT symptom A-6

page numbers 7-65
page titles 7-65
pair counts during capture 6-19
panel
active 7-31
menu 1-13
scrolling 7-30
zoom 7-52
PAP Wait 4-24
PAP wait A-5
parallel port 7-63
parameters— see startup parameters 11-22
path
DOS environment variable 11-6
pattern
AND, combining patterns 6-49
binary data 6-51
capture filter 6-46
character data 6-51
combination of four matchs 6-47
contexts of use 6-45
copy and paste 6-55
defining complex 6-46
don't match 6-50
example 6-55
hexadecimal data 6-51
joint effect of several patterns 6-57
logical combination of matches 6-47, 6-49
match example 6-50
offset 6-49, 7-47, 7-59
OR, choosing between patterns 6-49
pair of components 6-48
procedure for setting 6-53
search for frame 6-46, 7-59
trigger 6-46
X character 6-51
Pattern match capture filter 6-9, 6-34, 6-52
Pattern match display filter 7-6, 7-15
pattern trigger 6-9
pause
using F9 to pause 5-80
pausing capture 6-27, 6-74
PC Network
abbreviation in file name 11-5
available capture filters 6-34
filters for defective frames 6-58
Flip DLC address option 7-32
Highspeed mode option 6-9, 6-10, 6-32
internal trigger 6-62
network code in trace file 11-20
percent analyzed
field in Global Stats window 5-76
percentage bandwidth use
Global Stats fields 5-74
Physical err
Expert threshold 4-28
physical error
received 4-28
sent 4-28
physical layer
OSI vs. Expert layer 4-5
physical layer, OSI model 7-30
Physical level error
symptom A-11
playback, capture from file 6-11
Port unreachable
ICMP symptom A-9
presentation layer
OSI vs. Expert layer 4-5
presentation layer, OSI model 7-30
previous frame, function key 7-52
printer output
format 11-18
report 11-18
printing
capture buffer 7-61
destination 7-63
fields included 7-60
format 7-60
lines per page 7-66
overview 7-60
page range 7-63
page size 7-66
page titles 7-65

print options 7-62
printer port 7-63
to file 7-60
width of text 7-44
PRN, file extension for printer output 7-62
Proteon
and the Internetwork Analyzer 3-14
Proteon, manufacturer code 11-17
protocol
breakdown of traffic by family 5-73
field in summary window 5-42
filter
ARCNET network code 6-43
Ethertype 6-43
SAP 6-43
forcing 9-3
higher level address 7-9
higher level during capture 6-46
layers in detail view 7-45
layers in name table 11-15
undoing a forced protocol 9-13
Protocol capture filter 6-9, 6-34
Protocol display filter 7-6
protocol forcing 9-3
applying 9-10
applying a rule 9-10
available topologies 9-3
disabling 9-13
flag 7-41
how it works 9-3
specifying a rule 9-4
protocol interpreter 7-67
address format 7-46
available on Expert analyzer 2-20
bit level 7-67
Pyramid, manufacturer code 11-17

R

R flag 7-41
RAD Network Devices Ltd, manufacturer code 11-17
Read/write overlap
symptom A-4
Receive/Continue missing
symptom A-6
Receiver congestion error
MAC symptom A-13
Redirect network/host/frame
ICMP symptom A-9
reflectometer 6-4
Reinterpret option 7-55
REJ frame
WAN/Synchronous symptom A-15
Relative time display option 7-36, 7-43
relative utilization
field in statistics windows 5-68, 5-70
Remote xfer
Expert threshold 4-21
remove diag,F7 5-12
repeating a search 7-60
Reply retransmission
LAT symptom A-6
Request denied
symptom A-4
requests
field in summary window 5-42
Resolve names option 8-6, 11-13
resolving names with external files 8-9
Resp time
Expert threshold 4-18
restore diags,F8 5-12
restoring factory defaults 3-7, 11-13
resuming capture 6-28
Retix, manufacturer code 11-17
Retrans%
Expert threshold 4-22
Retransmissions
Diagnosis Detail display 5-33
Returned to ring
MAC symptom A-13
Reuse/Freeze allocation option 4-35
Reverse direction, option in address filter 6-43, 7-13
RI field 3-5, 6-51

generated frame 10-9
RI field, IEEE 802.3 10-10
Ridge, manufacturer code 11-17
Ring Beaconing
Diagnosis Detail display 5-34
MAC symptom/diagnosis A-13
ring beaconing
token ring counter 6-23
Ring entries
Expert threshold 4-28
Ring errors
Expert threshold 4-29
ring speed
setting for token ring 3-10
Rng purge dg
Expert threshold 4-30
Rng purge sy
Expert threshold 4-29
RNR frames
relation to congestion percentage 4-32
RNR frames capture filter 6-35, 6-60
root directory 11-6
Router buffer overflow
WAN/Synchronous symptom A-15
Router/Bridge frame type option 3-13
routers to subnet
field in subnet detail window 5-57
routing information
generated frame 10-9
RR frames
relation to congestion percentage 4-32
RR frames capture filter 6-35, 6-60
RS232
Internetwork Analyzer line interface 3-15
RS422
Internetwork Analyzer line interface 3-15
RS423
Internetwork Analyzer line interface 3-15
rule
applying for protocol forcing 9-10
for protocol forcing 9-4
run information
fields in Global Stats window 5-74
RX congestion 4-28

S

S flag 7-41
SAP
generated frame 10-3
protocol filter 6-43
Save at trigger option 6-67
Save names option 8-10
Save when full option 6-66, 6-67
saving
alphabetization in name table 11-15, 11-16
capture buffer 6-75, 8-11
capture filters 6-36
captured frames, effect of display filter 7-5
caution when saving name table 8-6, 8-11
current options in STARTUP file 8-22
display filters 7-27
edited name table 8-8
names to the name table 8-10
selected frames only 7-16, 8-12
setup file 8-23
setup files 6-36
trigger frame 6-66
scheduled events 3-19
Screen format option 6-9, 6-13
scrolling
in detail view 7-45
in display views 7-30
large capture buffer 7-31
synchronization between detail and hex 7-30
to next or previous frame 7-52
Scrolling Help menu 1-14
SDLC protocol 3-13
searching for
frame number 7-56
pattern 6-46, 7-59
text 7-58
Selected frame flag 7-41
Selected frames display filter 7-6, 7-16

selection menu
main 1-8
Sequent, manufacturer code 11-17
serial number of Sniffer analyzer B-3
service access point 6-43
session layer
OSI vs. Expert layer 4-5
session layer, OSI model 7-30
set mark, function key 7-51
setting
capture filters 6-35
capture filters for WAN/synchronous 6-61
display filters 7-7
display filters for good frames or frame defects 7-17
display filters,overview 7-4
interpretation in hex view 7-51
layers displayed in summary view 7-38
Name width display option 4-37
Network object display filter 7-18
pattern match capture filter 6-53
Pattern match display filter 7-16
Protocol capture filter 6-34
Protocol display filter 7-15
Selected frames display filter 7-16
source of capture 6-12
Station address display filter 7-12
Symptom frames filter 7-25
token ring speed 3-10
transceiver option for Model 70 3-8
trigger delay 6-68
trigger to stop capture 6-61, 6-63
setup file
contents 8-21
deleting 8-23
loading 8-23
saving 8-23
startup with customized options 11-12
Short flag 7-41
Short frames capture filter 6-34, 6-58
Short frames display filter 7-6, 7-17
signal loss
token ring counter 6-23
SilGrf, manufacturer code 11-17
Single Station
token ring counter 6-23
single station
token ring counter 6-23
size
capture buffer 6-7
effect of truncating frame 6-11
frame 6-10
generated frame 10-5
minimum frame 10-6
printed page 7-66
skyline view 6-14, 6-28
adjusting scales 6-30
units 6-15
SL, network abbreviation in file name 11-5
Slow File Transfer
Diagnosis Detail display 5-35
Slow file%
Expert threshold 4-21
Slow resp%
Expert threshold 4-18
Slow Server
Diagnosis Detail display 5-36
Small hello timer
DECnet symptom A-9
SNA 6-23, 6-26
SNIFF directory 11-7, 11-8, 11-12
SNIFF.CFG subdirectory 11-8
SNIFF.HLP file 11-7
Sniffer analyzer
role on network 1-5
starting in Expert mode 2-3
Sniffer Internetwork Analyzer
capture display options 6-14
setting capture filters 6-61
Sniffer Network Analyzer
main selection menu 1-8
major components 1-3
manuals xxxvi
SNSTART.BAT, passing startup parameters 11-22
source address
count 6-20

Source address is broadcast
symptom A-10
Source DLC address is broadcast
symptom A-11
Source quench
ICMP symptom A-10
source routing information 6-52
generated frame 10-9
spanned frames 7-49
effect of truncation 6-11
Specific (address) option 6-38
speed
token ring 3-12
Spider, manufacturer code 11-17
spread sheet
Delimited format option 11-18
format for 7-60
SSAP, example 10-15
stack
forcing protocol 9-3
standby monitor, token ring 1-5
StarLAN
address format 7-47
available capture filters 6-34
display filters 7-6
filters for defective frames 6-58
internal trigger 6-62
network code in trace file 11-20
start run
field in Global Stats window 5-75
starting
capture 6-74
traffic generator 10-13
startup
automatic use of files 11-12
startup files
initial setup 8-23
overview 11-12
related directories 11-12
types of 11-10
startup parameters 11-21
adapter card configuration 11-25
configuration of adapter card 11-25
context of use 11-24
editing 11-22
extended memory 11-25
specified in MNU files 11-22
STARTUP.xxD file 8-3, 8-5, 11-7
STARTUP.xxD, format of name table 11-13
STARTUP.xxI file 11-7
STARTUP.xxS file 3-7, 11-12
STARTUP.xxV
configuring for Expert analyzer 4-7
state
field in Global Symptoms detail window 5-60
station address 8-4
additional name table 11-13
display filter vs. capture filter 7-11
IEEE standard for bit order 7-67, 11-17
inclusion of manufacturer ID 11-16
name table 7-14, 11-15
name table field 11-14
symbolic equivalent 8-3
traffic generator 10-5
width of display field 4-37, 7-34
Station address capture filter 6-9, 6-34, 6-39
Station address display filter 7-5, 7-6, 7-11
considerations 7-14
station name
editing 8-6
Station off ring
MAC symptom A-13
station status
field in token ring statistics windows 5-71
Statistics window
application layer 5-63
connection layer 5-65
DLC Station layer 5-68
Expert analyzer 2-18
network station layer 5-67
overview 5-6
symptom and network object 5-60
to display 5-61
Stn removed

Expert threshold 4-29
Stop at trigger option 6-9, 6-62, 6-64
Stop capture option 6-64
Stop when full option 6-9
stopping
capture 6-28, 6-61, 6-74
capture with trigger 6-61
traffic generator 10-14
subnet
detail window for subnet pairs 5-56
field in summary windows 5-49
Summary window 5-49
subnet mask
default Expert masks 4-8
subnet masks
configuration 4-7
non-standard 4-8
summary view 7-27, 7-33
role in protocol forcing 9-4
with detail view 7-45
summary view display options 7-35
Summary window
available formats 5-45
displaying 5-39
Global Symptom 5-50
information in 2-16, 5-40
meaning of asterisk 5-11
overview 5-5, 5-38
subnet counts 5-49
Sun Yellow Pages
learning names 4-38
Sun, manufacturer code 11-17
Symblx, manufacturer code 11-17
symptom
and the Expert analyzer 2-4
defined 2-4
Detail windows 5-52
display filter 7-24
field in subnet detail window 5-57
field in subnet summary window 5-49
field in summary window 5-43
getting more information 2-16
listed at application layer A-3
listed at connection layer A-4
listed at DLC Station layer A-11
listed at MAC layer A-11
listed at network station layer A-7
listed for Internetwork analyzer A-13
overview of related displays 2-16
related Expert displays 5-38
setting thresholds for 4-13
Statistics windows 5-60
Summary displays 5-38
using as a filter 7-17
Symptom frames filter 7-24
symptoms
column in Expert Overview 5-8
Synchronization frame missing
symptom A-6
synchronization of views 7-67
system options
all items in Options menu (whole chapter) 3-3
Sytek, manufacturer code 11-17

T

T flag 6-63, 7-40
T1
interface for Internetwork Analyzer 3-15
tabular view 6-14
TCP
byte rather than packet-oriented 6-11
example 7-45
example of pattern match 6-50
IP protocol number 6-56
Telnet code 6-56
TCP keep alive
Expert threshold 4-23
TCP/IP
learning names 4-38
pattern match example 6-55
setting IP addresses 4-7
setting subnet masks 4-7
TDR
as part of cable test 3-7

Technical Support xl
fax number B-3
phone number B-3
Tektronix, manufacturer code 11-17
TeleSniffer
Remote2 11-8
Telnet
pattern match example 6-55
TCP code 6-56
terminology
Expert analyzer 2-3
in Sniffer manuals xxxviii
text, interpretation in hex view 7-51
thermometer
units 6-15
this screen intentionally blank
screen message 6-24
thresholds
at DLC Station layer 4-25
at MAC layer 4-28
at network station layer 4-24
Broadcast dg 4-27
Broadcast sy 4-27
Congestion percentage 4-32
DEC hello 4-24
DEC keep alive 4-23
Denied count 4-19
Denied req% 4-20
Duplicate% 4-24
effects of changing 4-15, 4-32
Expert application layer 4-18
Fast retrans 4-23
Filter time 4-19
for Internetwork Analyzer 4-30
for token ring 4-28
for WAN/Synchronous 4-30
Idle timer 4-23
interaction of thresholds 4-16
LAN overload 4-26
LAN overload% 4-26
Local xfer 4-21
Loop% 4-20
Min appl req 4-18
Mult routers 4-24
No responses 4-22
on token ring 4-28
Overload timer 4-31
Physical err 4-28
Remote xfer 4-21
Resp time 4-18
Retransmission% 4-22
Ring entries 4-28
Ring errors 4-29
Rng purge dg 4-30
Rng purge sy 4-29
RX congestion 4-28
setting on Expert analyzer 4-13
Slow file% 4-21
Slow resp% 4-18
Stn removed 4-29
TCP keep alive 4-23
Underload timer 4-31
WAN Overload 4-30
WAN Underload 4-31
Zero window 4-22
throughput
field in statistics window 5-64
TI, manufacturer code 11-17
time
format in trace file 11-19, 11-20
unit, field in trace file 11-19, 11-20
time-domain reflectometer 6-4
timestamp
and the LM2000-Internetwork Analyzer conversion utility 8-16
Time-to-live exceeded
symptom A-10
Time-to-live expiring
IP symptom A-10
title, printed report 7-65
Token error
MAC symptom A-13
token ring
active monitor in traffic generation 10-13
address format 7-47

address recognized bits 7-71
available Expert triggers 6-72
data field within frame 10-10
DLC address 7-33
Expert thresholds 4-28
Expert thresholds for 4-28
fragmented or beaconing 3-12
frame copied 7-71
generic address format 6-39
LAN Manager functional address 1-5
list of diagnoses A-18
list of symptoms A-11
location in ring 7-71
monitor 1-5
network code in trace file 11-20
No signal-remove option 3-11
ring beaconing counter 6-23
signal loss counter 6-23
single station counter 6-23
special counters during capture 6-22
speed 3-10, 3-12
system options 3-8
trace tool present" 1-5
trailer 7-71
trigger example 6-65
xmit beacon counter 6-23

Token Ring-II
counters during capture 6-22
setting network speed 3-11
size of generated frames 10-6

Token Ring-III
and the lost frames counter 6-23
counters during capture 6-23
setting network speed 3-11

TOOLS, directory 11-7

total bytes
field in statistics window 5-66

total file transfers
field in statistics window 5-63

total symptoms
field in detail windows 5-56

T-POD
and the Internetwork Analyzer 3-15

trace file
captured frames 6-75
contents 11-19
conversion between LM2000 and Internetwork Analyzer 8-14
end of file record 11-21
format 11-8, 11-18
header 11-19
limitation of capturing from 6-12
name 11-8
source of capture 6-11
version record 11-19

trace tool present, token ring message 1-5

traffic
total 6-28

traffic density, bar graph during capture 6-17

traffic generator 1-5
bar graph of transmission rate 10-13
frame content 10-14
frame format 10-14
frame size 10-5
interval between frames 10-6
specifying destination 10-5
specifying length of RI field 10-9
specifying number of frames to generate 10-7
specifying the data field 10-7
starting 10-13
stopping 10-14
use with RI fields 10-9

traffic, total 6-18

trailer, token ring 7-71

transmission order
bits within byte 7-66, 11-17
high-order-bit first 11-17
low-order-bit first 11-17
variation by network 7-66

transport
OSI vs. Expert layer 4-5

transport layer, OSI model 7-30

Transport retransmission
symptom A-6

trigger
available MAC layer Expert triggers 6-72

defective frames 6-9
defining 6-63
delay 6-9
disabling temporarily 6-69
effects of an Expert trigger 6-71
event, defined 6-62
example
Ethernet 6-65
token ring 6-65
Expert token ring triggers 6-72
Expert triggers 6-69
Expert triggers at application layer 6-72
Expert triggers at connection layer 6-72
Expert triggers at DLC Station layer 6-72
Expert triggers at network station layer 6-72
Expert vs. Classic triggers 6-73
external 6-9
frame identified with flag 6-62
marking of trigger frame 6-73
pattern 6-9, 6-46
procedure to set 6-64, 6-65
processing order 6-73
setting 6-61
using diagnoses as triggers 6-69
Trigger flag 6-62, 7-40
Trigger position 6-9
Trigger position option 6-66
TRLR, protocol filter 6-45
troubleshooting B-3, B-6
truncation
effect on spanned frame 6-11
truncation of frames 6-10
trustee names
setting on Expert analyzer 4-12
TRW, manufacturer code 11-17
Two viewports display option 7-28
Two-station format
display option 7-36, 7-39
example 7-39
type
station address in name table 11-15

U

U-B, manufacturer code 11-17
Underload timer
Expert threshold 4-31
Underloaded Network
diagnosis 4-31
diagnosis detail display 5-37
WAN/Synchronous diagnosis A-19
Ungermann-Bass
and the Internetwork Analyzer 3-14
Unisys, manufacturer code 11-17
units
counters,totals, skylines, density bar graph 6-15
Univation, manufacturer code 11-17
Unknown stations only capture filter 6-9, 6-34, 6-37, 6-38
upstream neighbor
field in token ring statistics windows 5-71
upstream neighbor, token ring 7-71
Use defaults command 3-7, 6-36, 11-13
resetting Expert thresholds 4-14

V

V.10
Internetwork Analyzer line interface 3-15
V.11
Internetwork Analyzer line interface 3-15
V.35
Internetwork Analyzer line interface 3-15
validity checks 7-71
version field in trace file 11-19
version record 11-19
view
detail 7-27, 7-44, 7-45
hex 7-47
scrolling 7-30
summary 7-27, 7-33
VINES, bit-level interpretation 7-68
VIP, example of bit-level interpretation 7-68
Visual Technology, manufacturer code 11-17

Vitalink
and the Internetwork Analyzer 3-14
Vitalink, manufacturer code 11-17
void frame capture filter 6-34

W

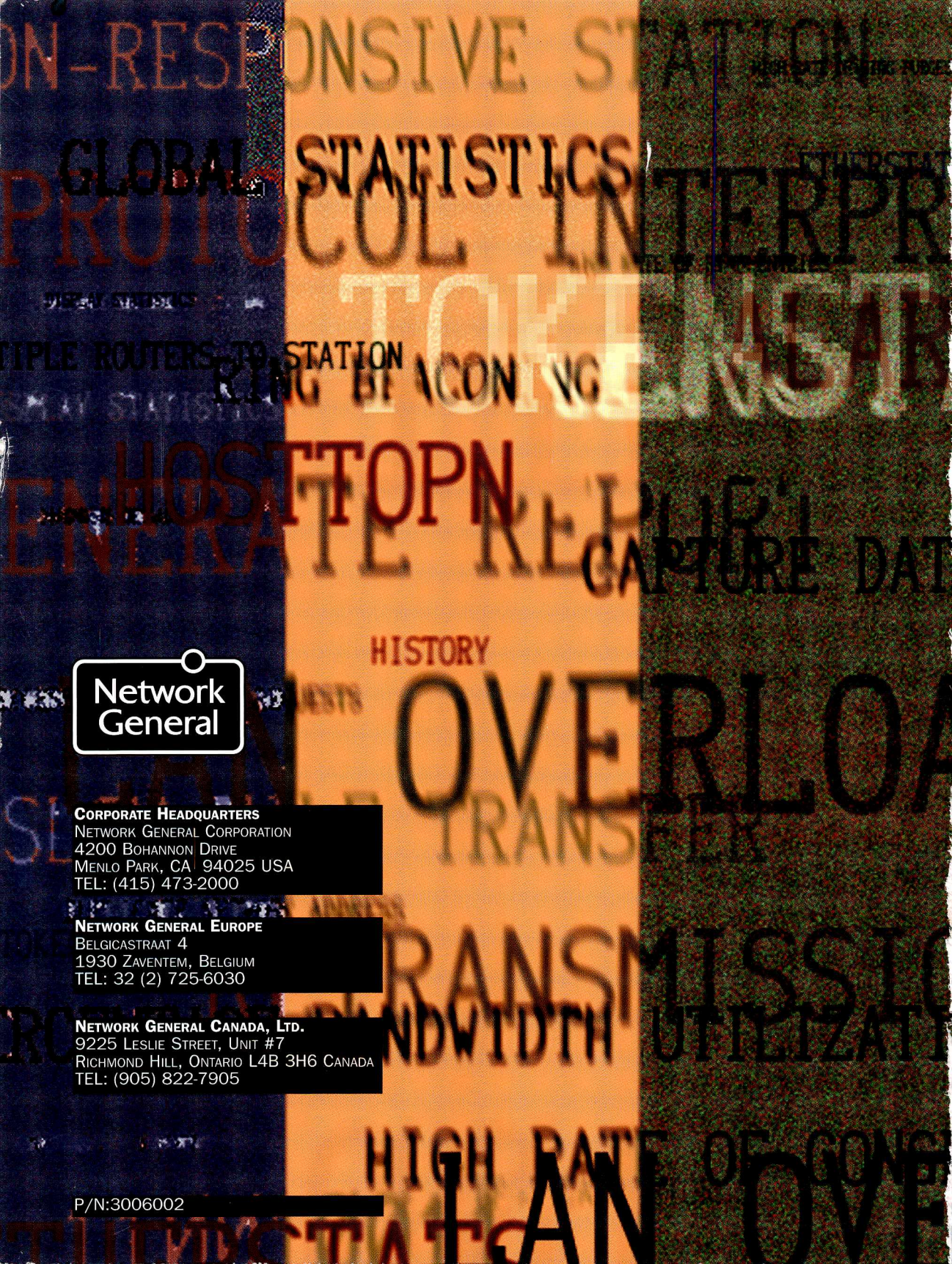
WAN congested
WAN/Synchronous symptom A-15
WAN Overload
Expert threshold 4-30
WAN overloaded
WAN/Synchronous diagnosis A-19
WAN Underload
Expert threshold 4-31
WAN/Synchronous symptom A-15
WAN/Synchronous
Expert thresholds 4-30
list of diagnoses A-19
list of symptoms A-13
WAN/synchronous
Abort flag 7-41
active vs. completed calls 6-27
capture display options 6-14
capture filters 6-35
encoding methods 3-15
frame counts during capture 6-23
frame sequence numbers 3-15
Frame type options 3-13
frames seen reported 6-28
function keys during capture 6-27
indicators of line status 6-24, 6-30
internal trigger 6-62
Invert option 3-15
logical calls 6-26
naming addresses 6-27
network code in trace file 11-20
setting trigger to stop capture 6-65
traffic density bar graphs 6-23
wrong frame type displayed 3-14
Wellfleet
and the Internetwork Analyzer 3-14
Wellfleet, manufacturer code 11-17
Western Digital, manufacturer code 11-17
Window frozen
TCP/IP symptom A-6
Window size exceeded
TCP/IP symptom A-6
Wrong reply sequence
symptom A-6

X

X flag 7-41
X Windows
protocol,spanned frames 6-11
X.25 6-23, 6-26
X.400
address level 7-9
syntactic vs. semantic interpretation 7-69
Xerox, manufacturer code 11-17
xmit beacon
token ring counter 6-23
XNS
address format 7-47
address level 7-9
Xyplex, manufacturer code 11-17
Xyvision, manufacturer code 11-17

Z

Zero window
Expert threshold 4-22
TCP/IP symptom A-6
Zeros broadcast address
IP symptom A-10
ZIP Storm 4-27, A-11
ZNet
network code in trace file 11-20
zoom
function key 7-52



Network General

Corporate Headquarters
Network General Corporation
4200 Bohannon Drive
Menlo Park, CA 94025 USA
TEL: (415) 473-2000

Network General Europe
Belgicastraat 4
1930 Zaventem, Belgium
TEL: 32 (2) 725-6030

Network General Canada, Ltd.
9225 Leslie Street, Unit #7
Richmond Hill, Ontario L4B 3H6 Canada
TEL: (905) 822-7905

P/N:3006002